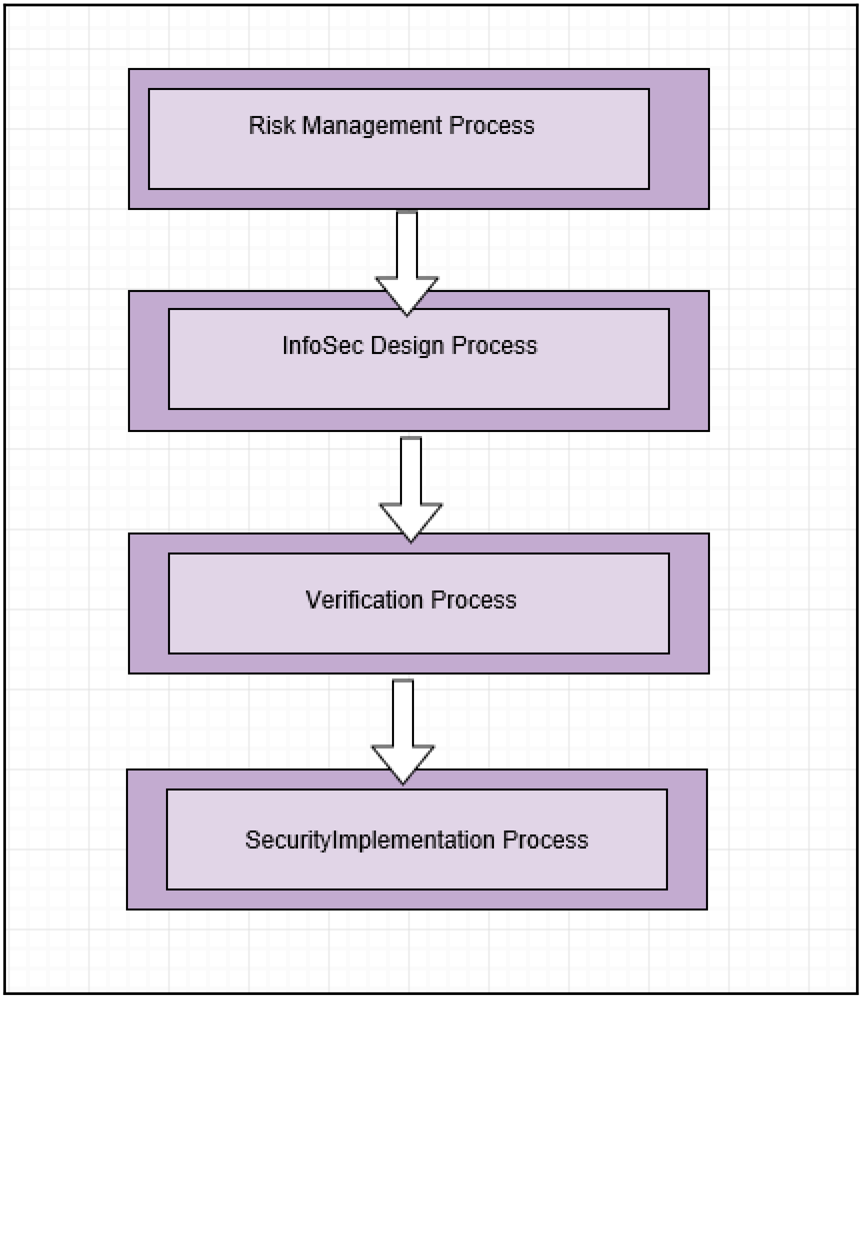
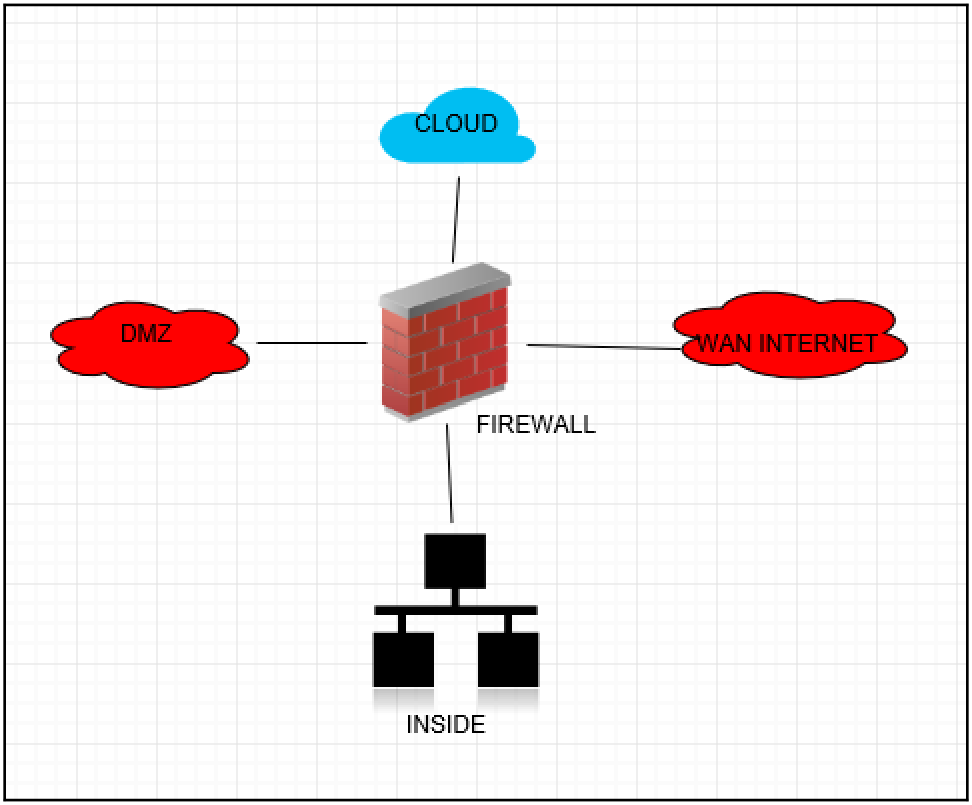
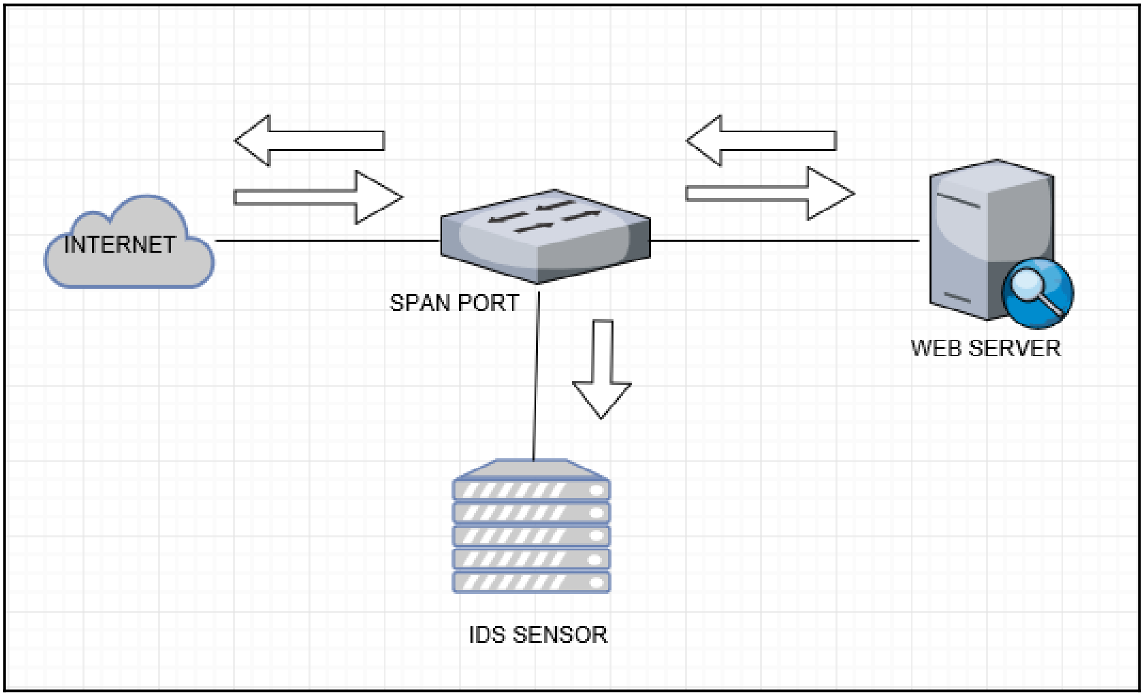
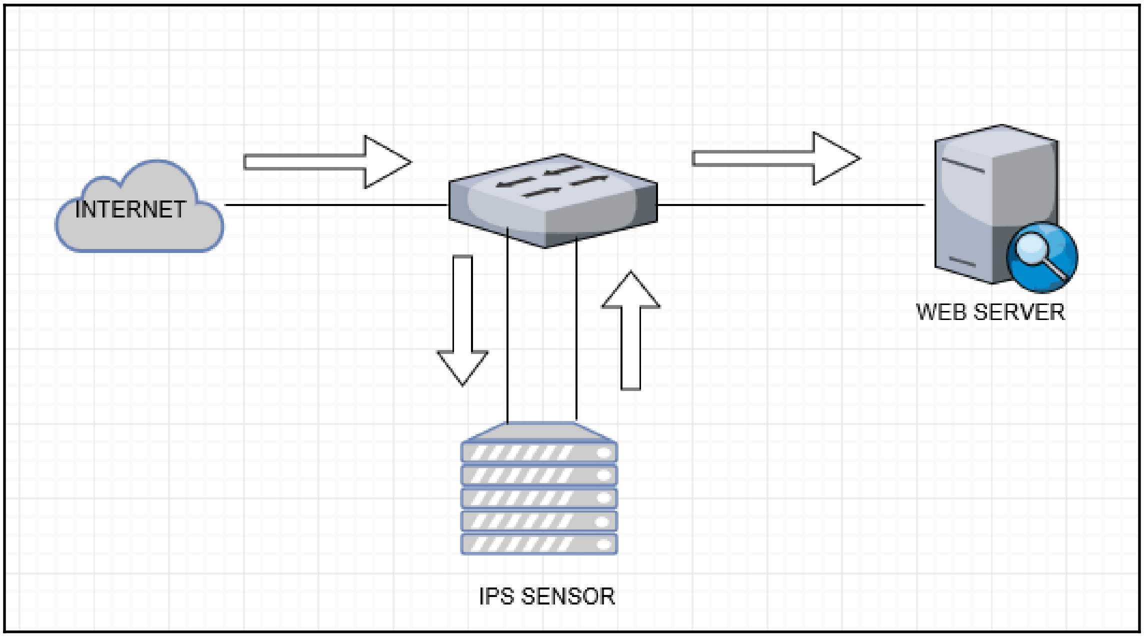
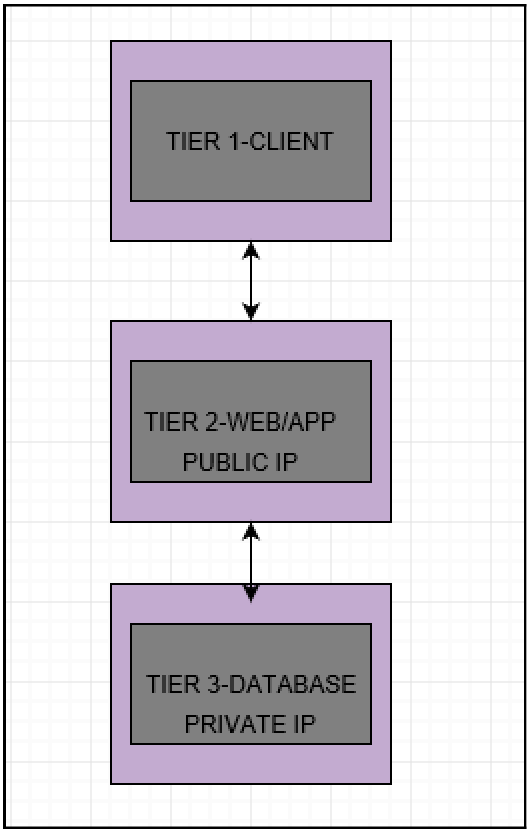
Chapter 1: Fundamental Security Concepts

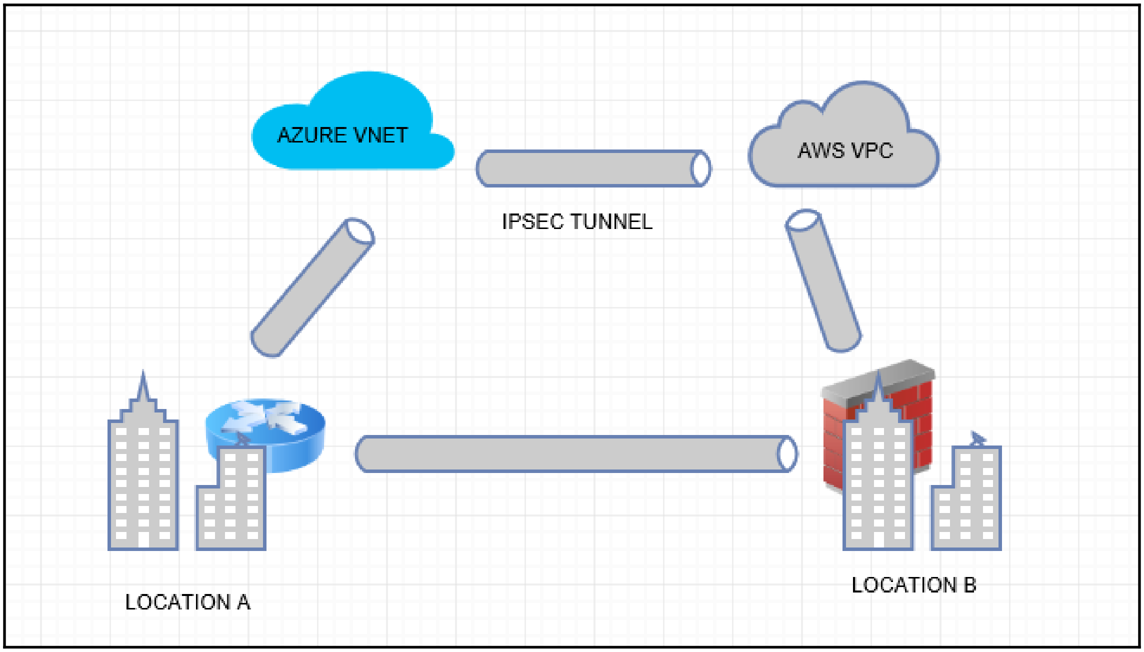


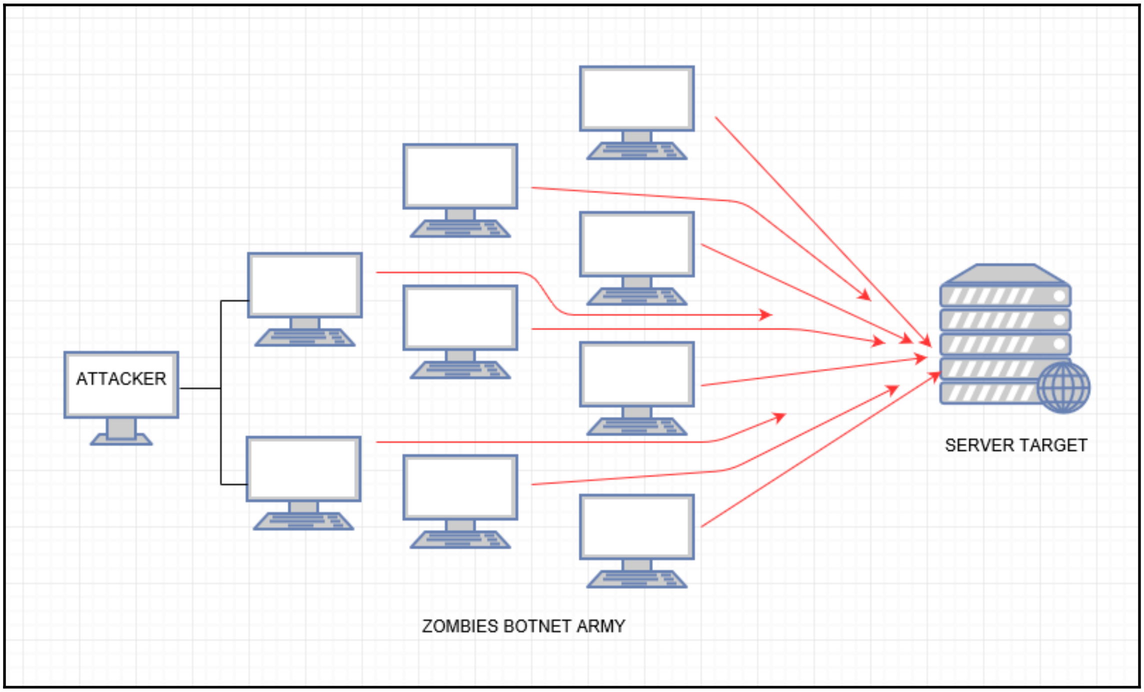

CLOUD
DMZ
WAN INTERNET
FIREWALL
INSIDE

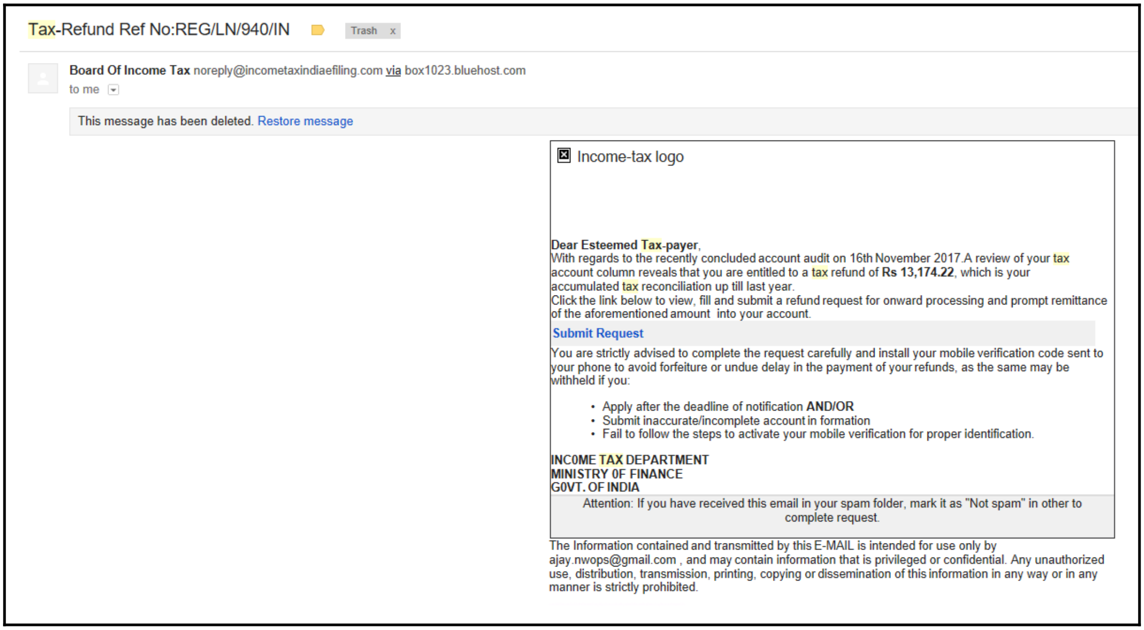

INTERNET
SPAN PORT
WEB SERVER
IDS SENSOR


INTERNET
WEB SERVER
IPS SENSOR


TIER 1-CLIENT
TIER 2-WEB/APP
PUBLIC IP
TIER 3-DATABASE
PRIVATE IP


AZURE VNET
AWS VPC
IPSEC TUNNEL
LOCATION A
LOCATION B


ATTACKER
SERVER TARGET
ZOMBIES BOTNET ARMY



Tax-Refund Ref No:REG/LN/940/IN

Board Of Income Tax noreply@incometaxindiaefiling.com via box1023.bluehost.com

This message has been deleted. Restore message

☒ Income-tax logo

Dear Esteemed Tax-payer,
With regards to the recently concluded account audit on 16th November 2017.A review of your tax account column reveals that you are entitled to a tax refund of **Rs 13,174.22**, which is your accumulated tax reconciliation up till last year.
Click the link below to view, fill and submit a refund request for onward processing and prompt remittance of the aforementioned amount into your account.

Submit Request

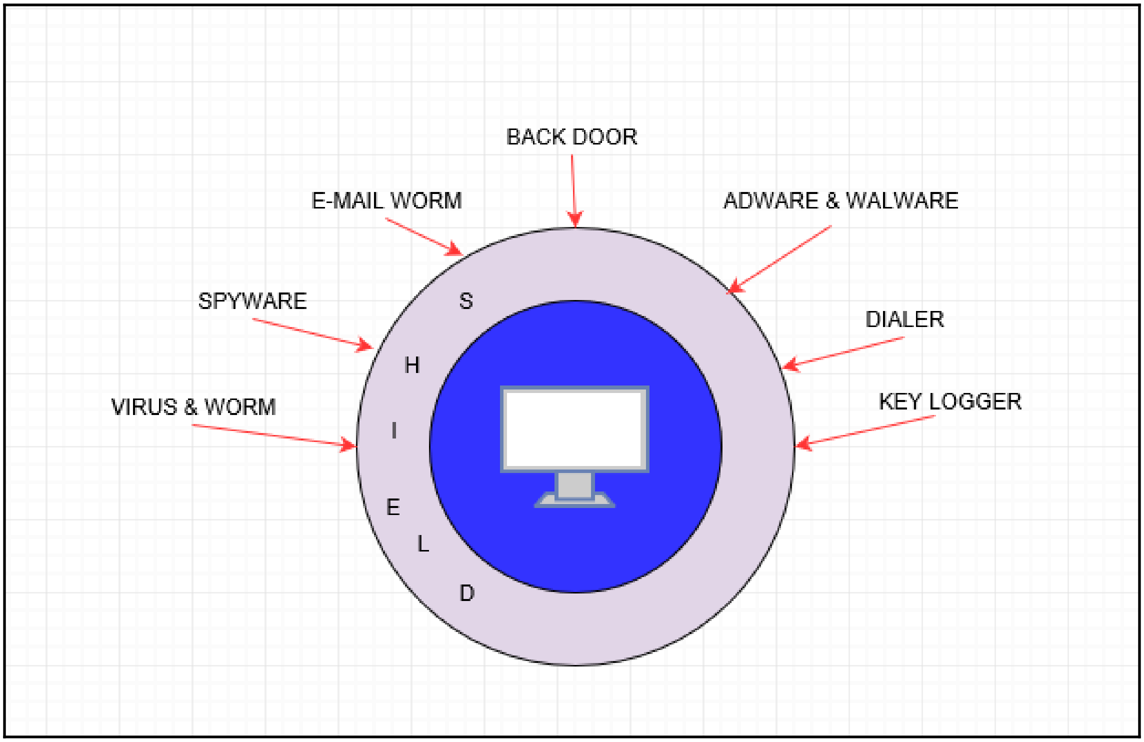
You are strictly advised to complete the request carefully and install your mobile verification code sent to your phone to avoid forfeiture or undue delay in the payment of your refunds, as the same may be withheld if you:

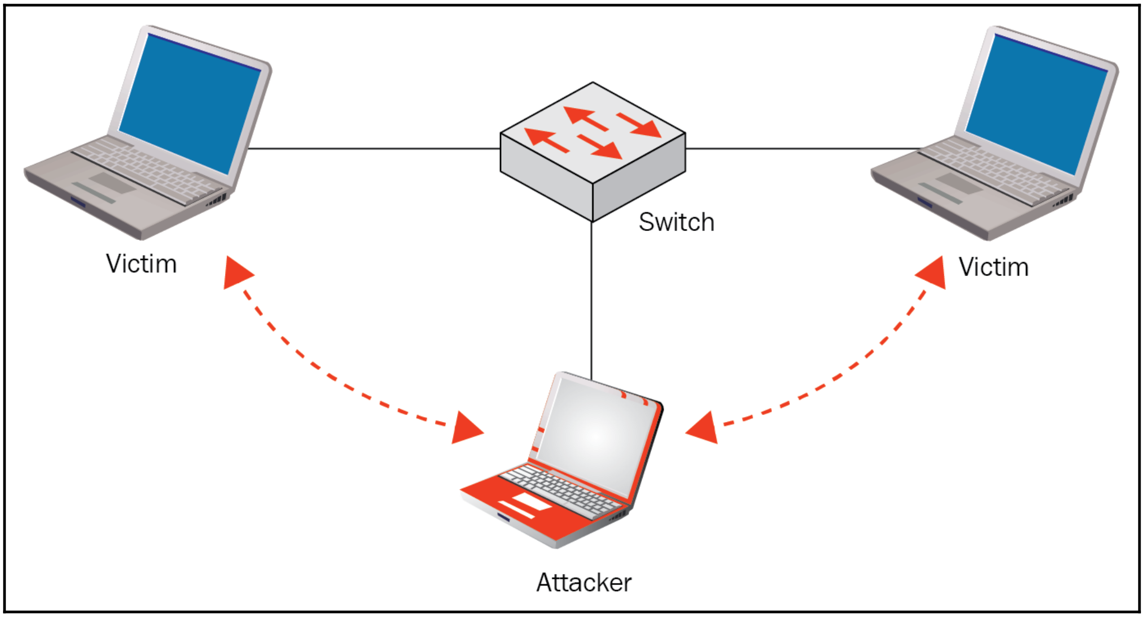
- Apply after the deadline of notification **AND/OR**
- Submit inaccurate/incomplete account in formation
- Fail to follow the steps to activate your mobile verification for proper identification.

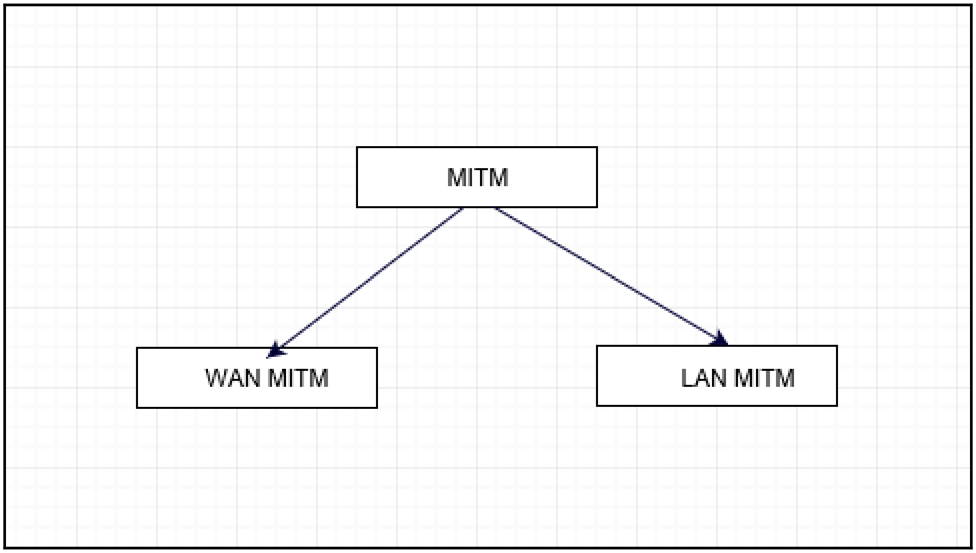
INC0ME TAX DEPARTMENT
MINISTRY 0F FINANCE
G0VT. OF INDIA

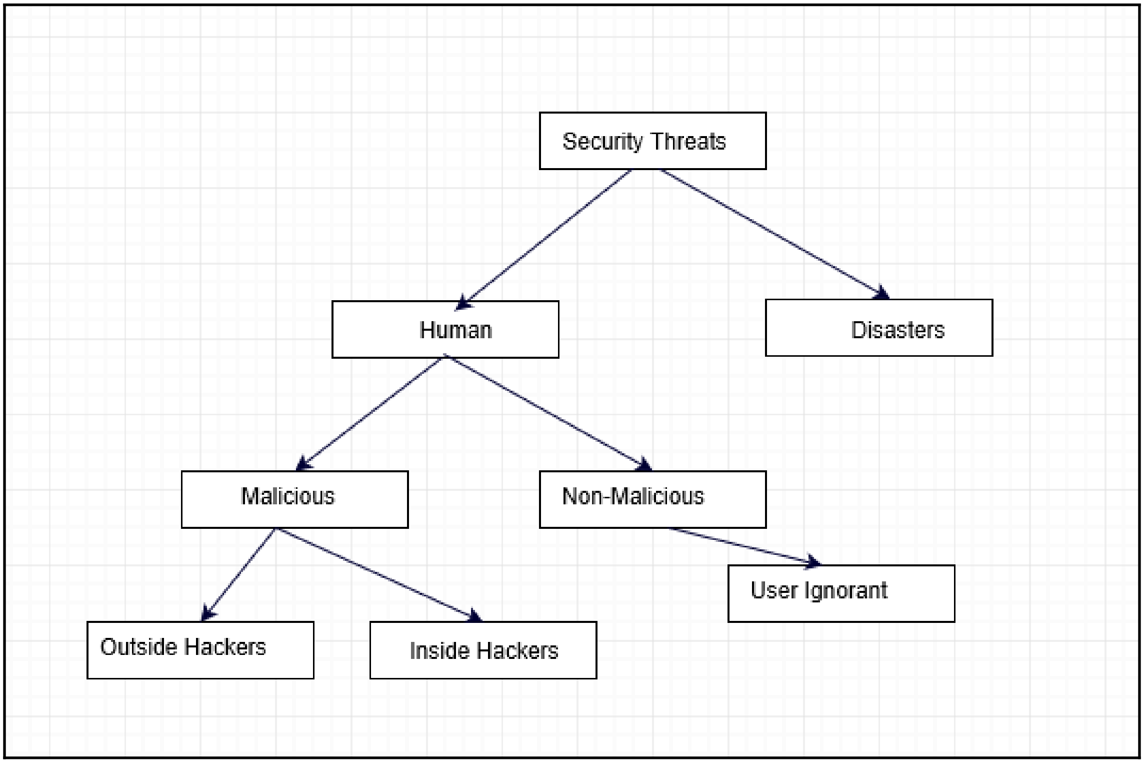
Attention: If you have received this email in your spam folder, mark it as "Not spam" in other to complete request.

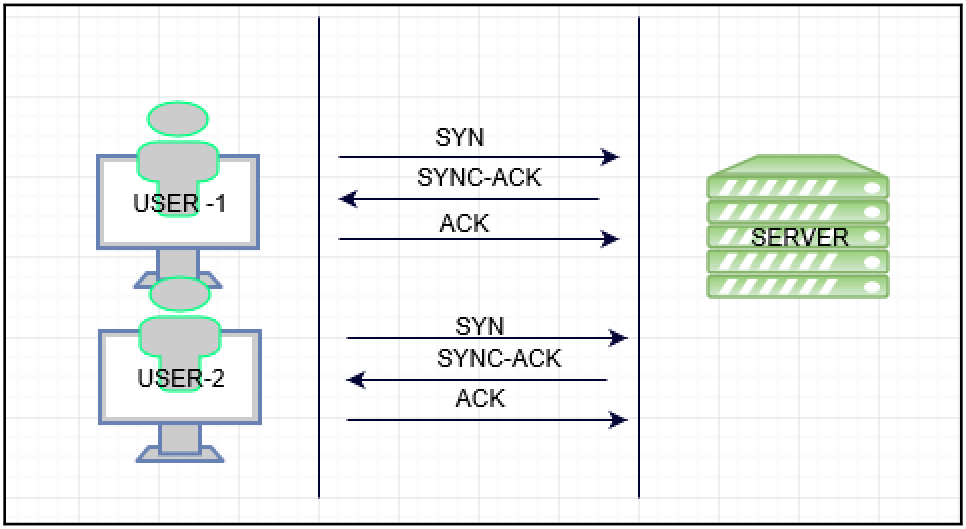
The Information contained and transmitted by this E-MAIL is intended for use only by ajay.nwops@gmail.com , and may contain information that is privileged or confidential. Any unauthorized use, distribution, transmission, printing, copying or dissemination of this information in any way or in any manner is strictly prohibited.

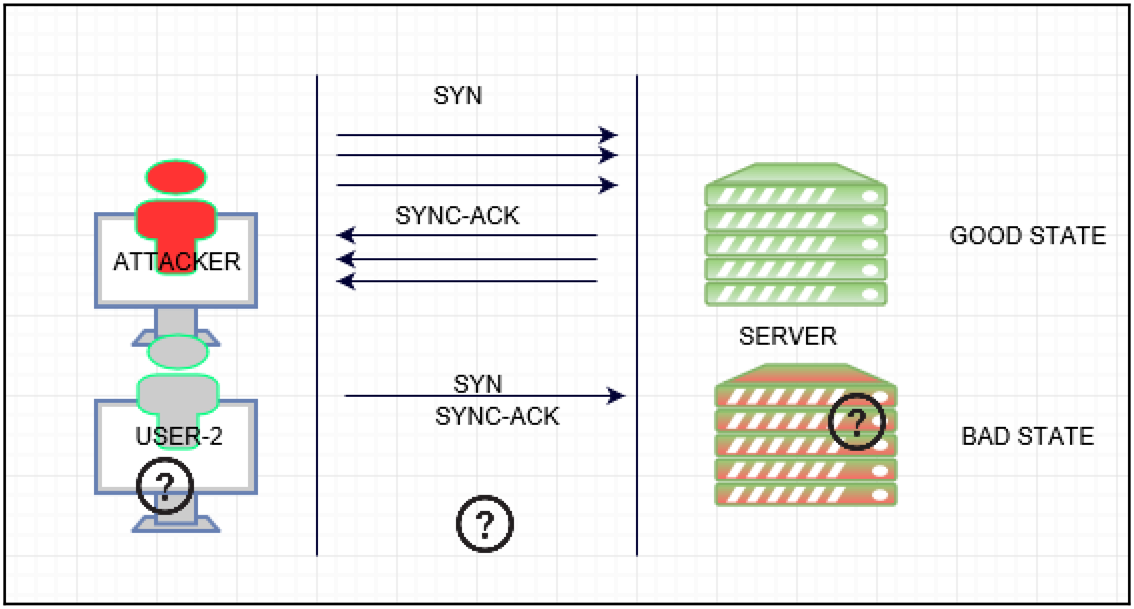

BACK DOOR
E-MAIL WORM
ADWARE & WALWARE
SPYWARE
DIALER
KEY LOGGER
VIRUS & WORM
S
H
I
E
L
D


Victim
Switch
Victim
Attacker


MITM
WAN MITM
LAN MITM

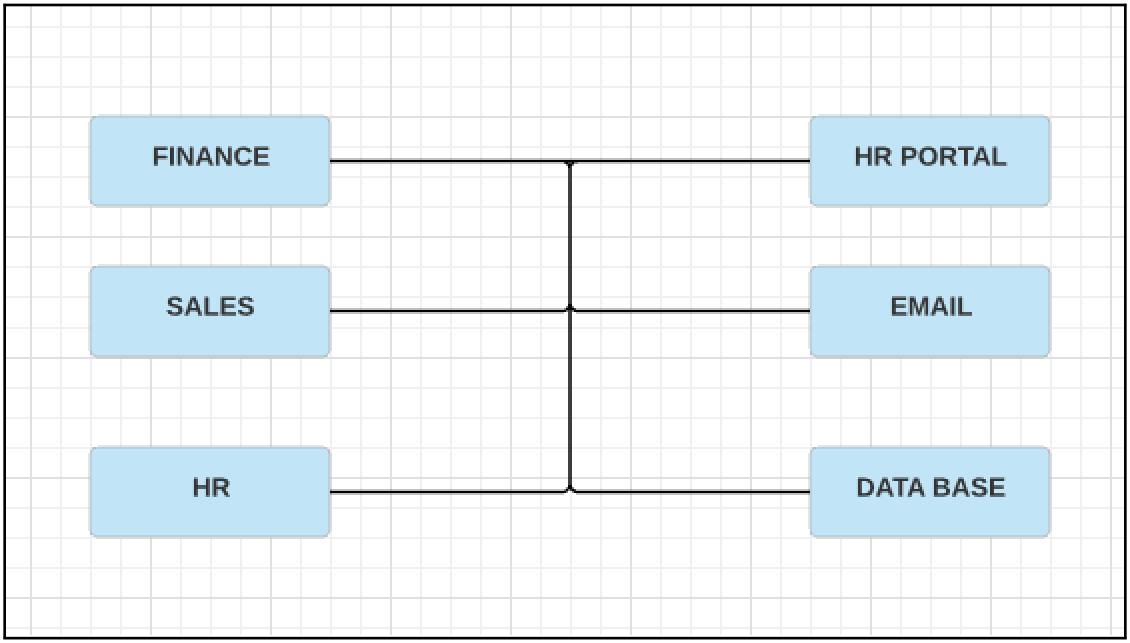

Security Threats
Human
Disasters
Malicious
Non-Malicious
User Ignorant
Outside Hackers
Inside Hackers

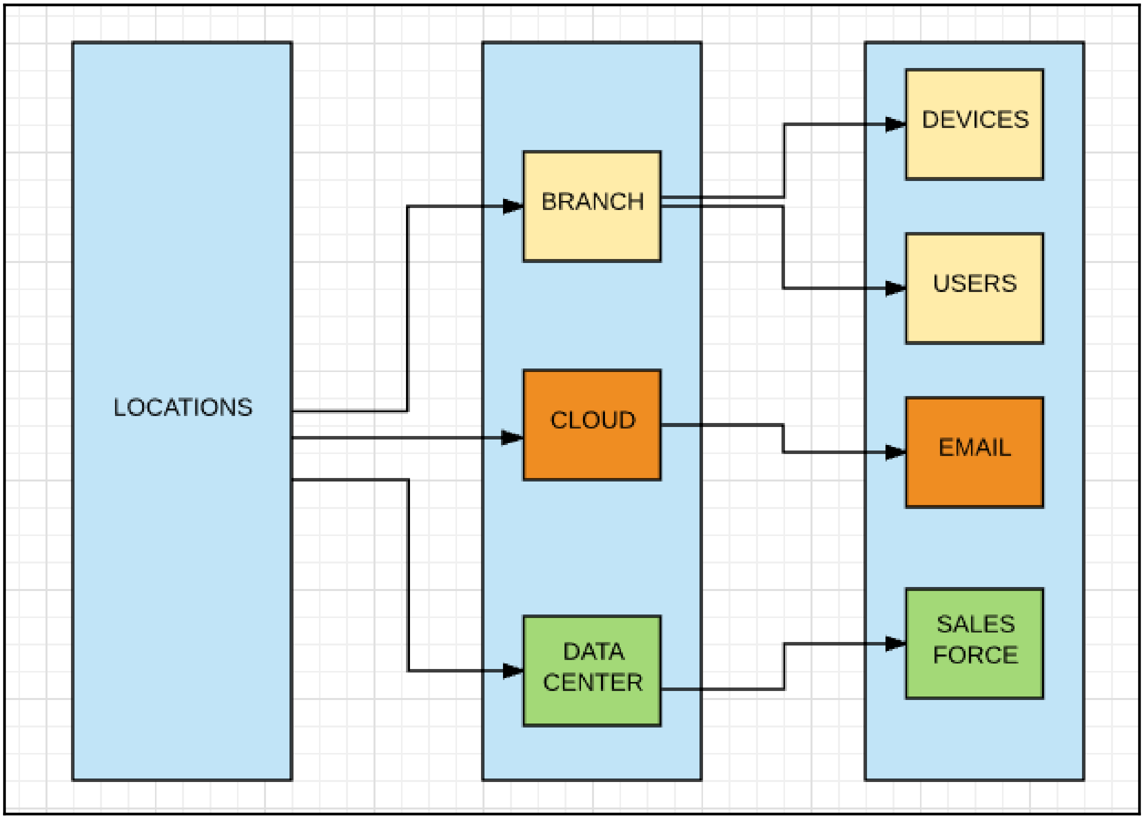

USER -1
USER-2
SYN
SYNC-ACK
ACK
SYN
SYNC-ACK
ACK
SERVER

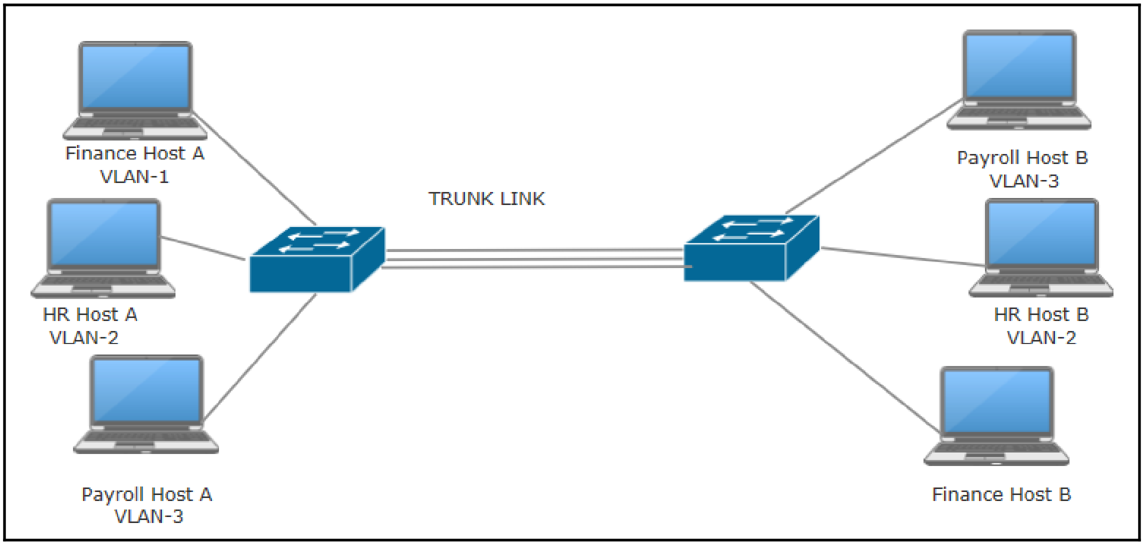

ATTACKER
USER-2
SYN
SYNC-ACK
SYN
SYNC-ACK
?
?
?
SERVER
GOOD STATE
BAD STATE

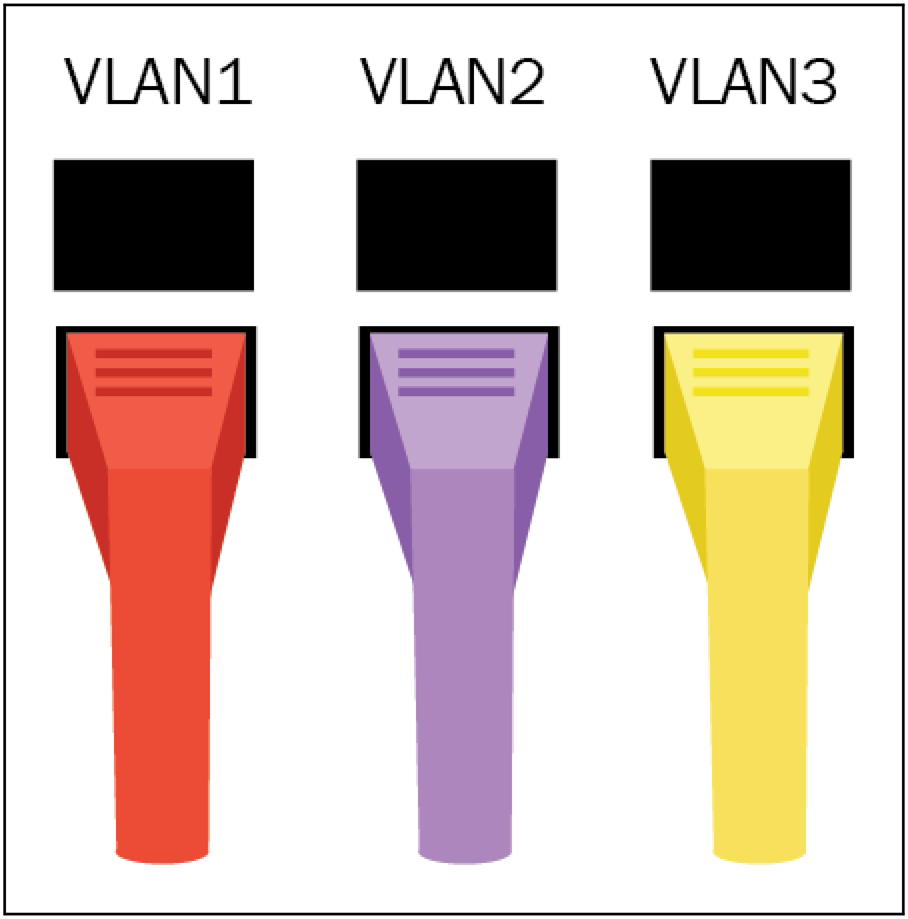
Free WiFi
Hijacked

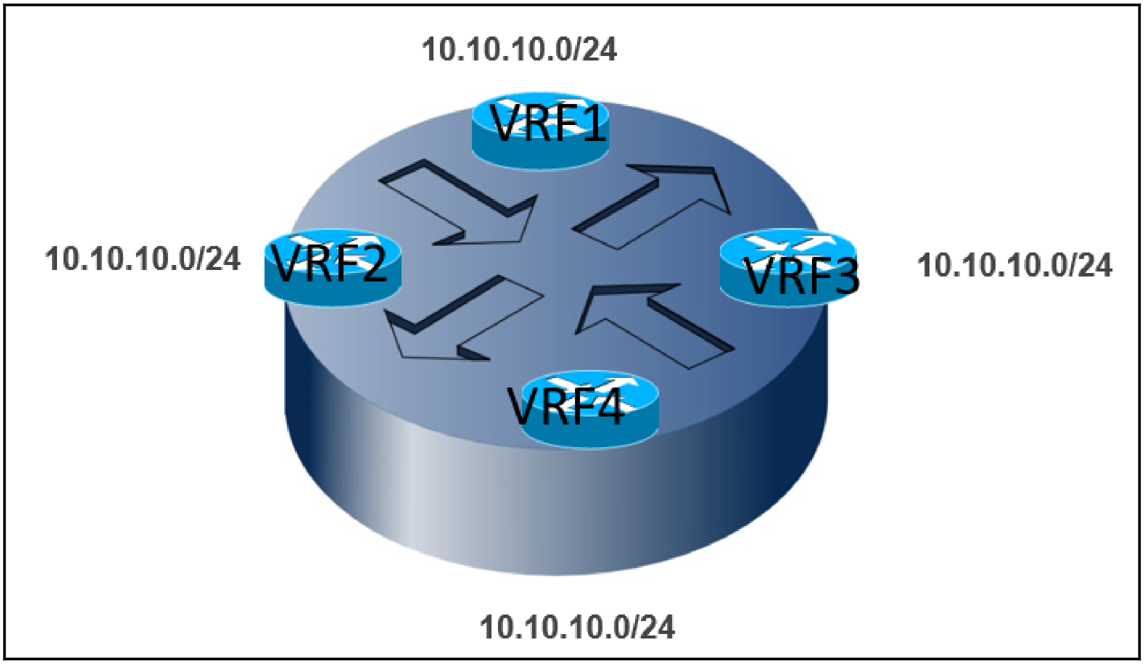
Chapter 2: Secure Network Design

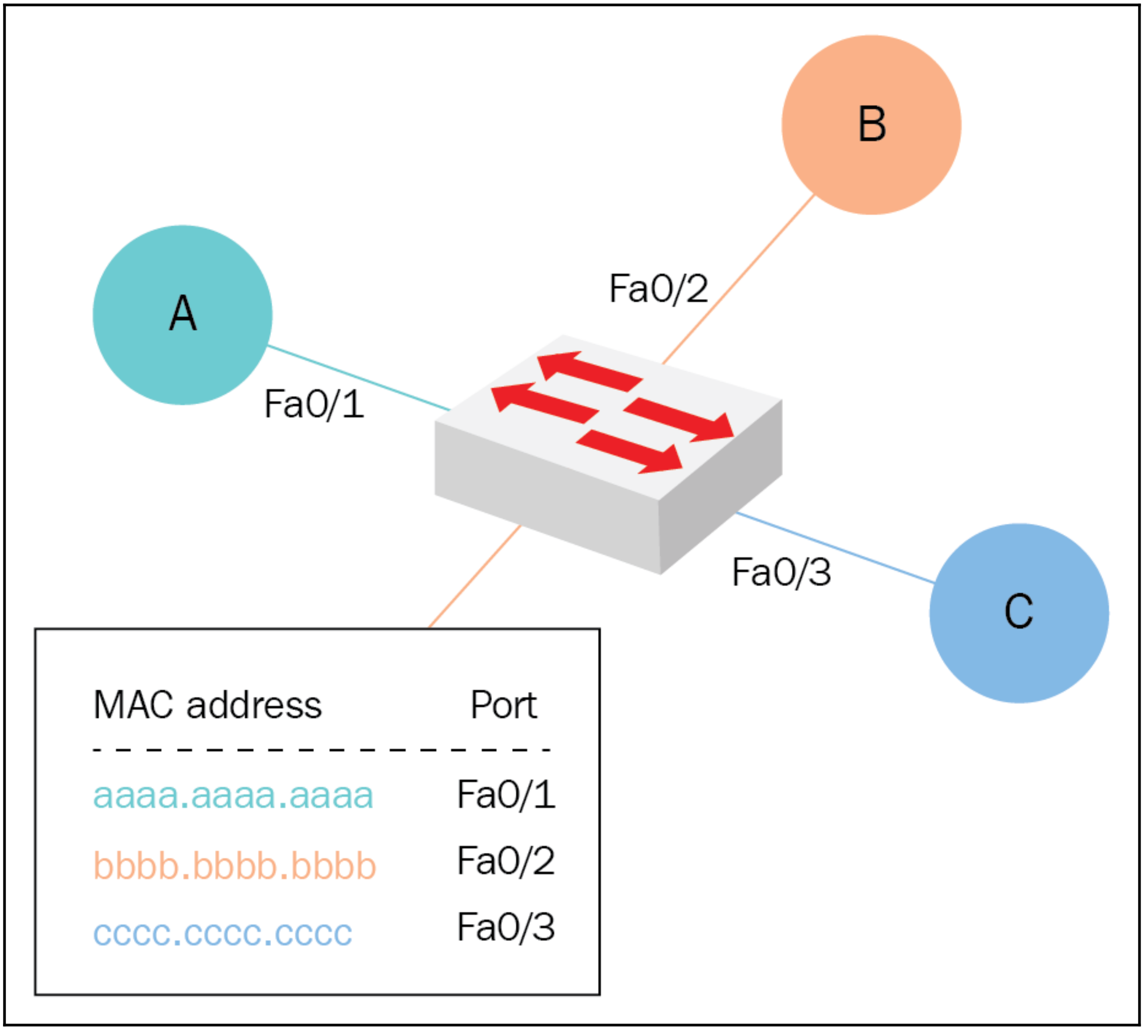



LOCATIONS
BRANCH
CLOUD
DATA CENTER
DEVICES
USERS
EMAIL
SALES FORCE

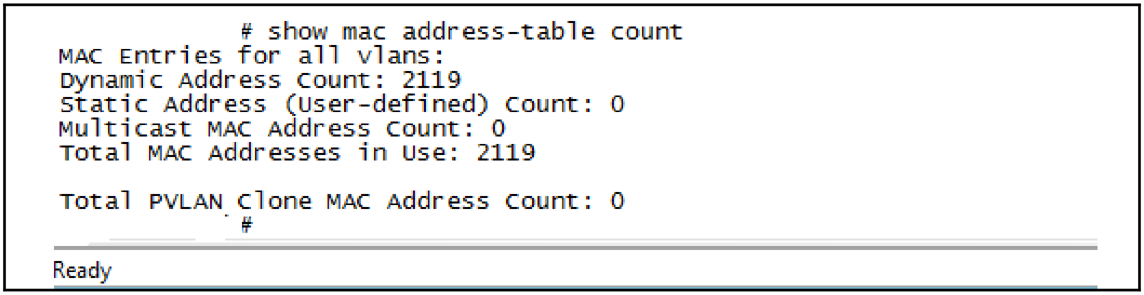

Finance Host A
VLAN-1
HR Host A
VLAN-2
Payroll Host A
VLAN-3
TRUNK LINK
Payroll Host B
VLAN-3
HR Host B
VLAN-2
Finance Host B


VLAN1
VLAN2
VLAN3

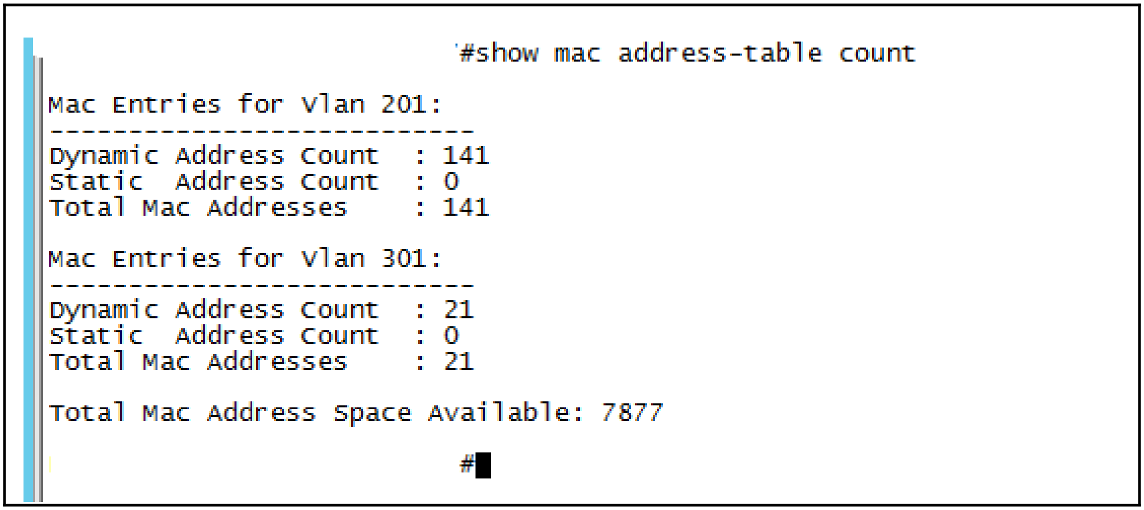

10.10.10.0/24
VRF1
10.10.10.0/24
VRF2
VRF3
10.10.10.0/24
VRF4
10.10.10.0/24



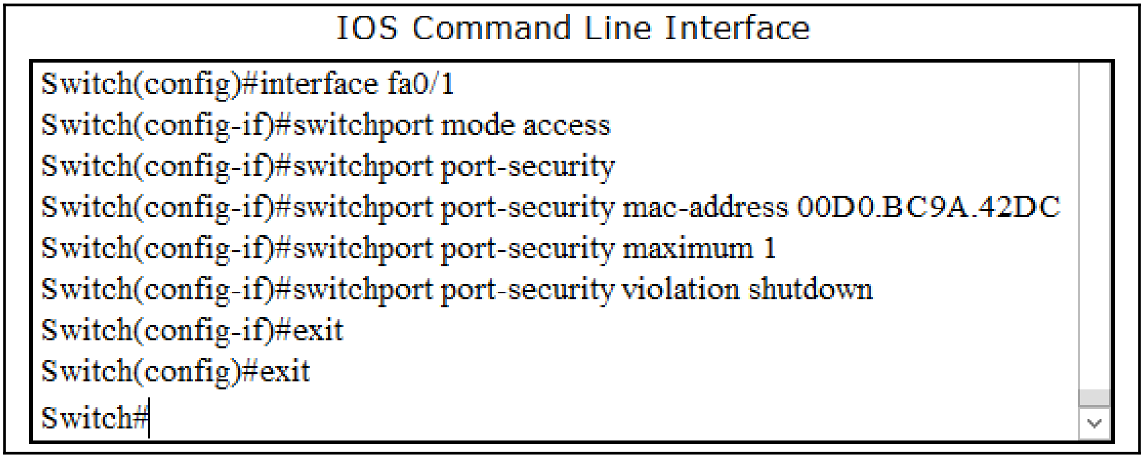
MAC address	Port
aaaa.aaaa.aaaa	Fa0/1
bbbb.bbbb.bbbb	Fa0/2
cccc.cccc.cccc	Fa0/3



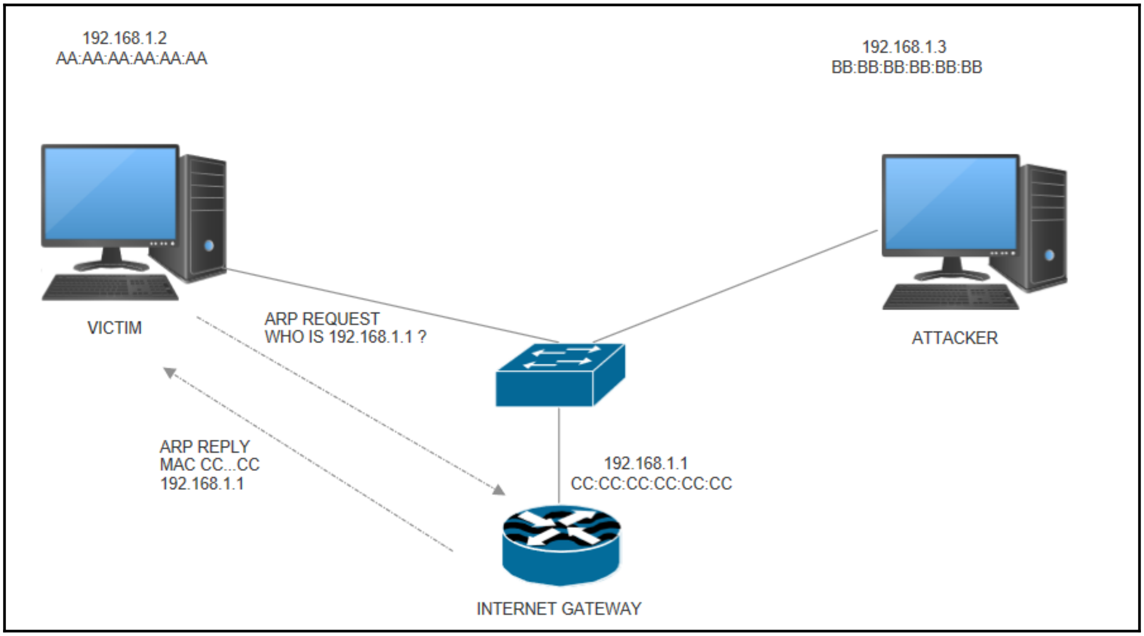
```
              # show mac address-table count
MAC Entries for all vlans:
Dynamic Address Count: 2119
Static Address (User-defined) Count: 0
Multicast MAC Address Count: 0
Total MAC Addresses in Use: 2119

Total PVLAN Clone MAC Address Count: 0
              #
```

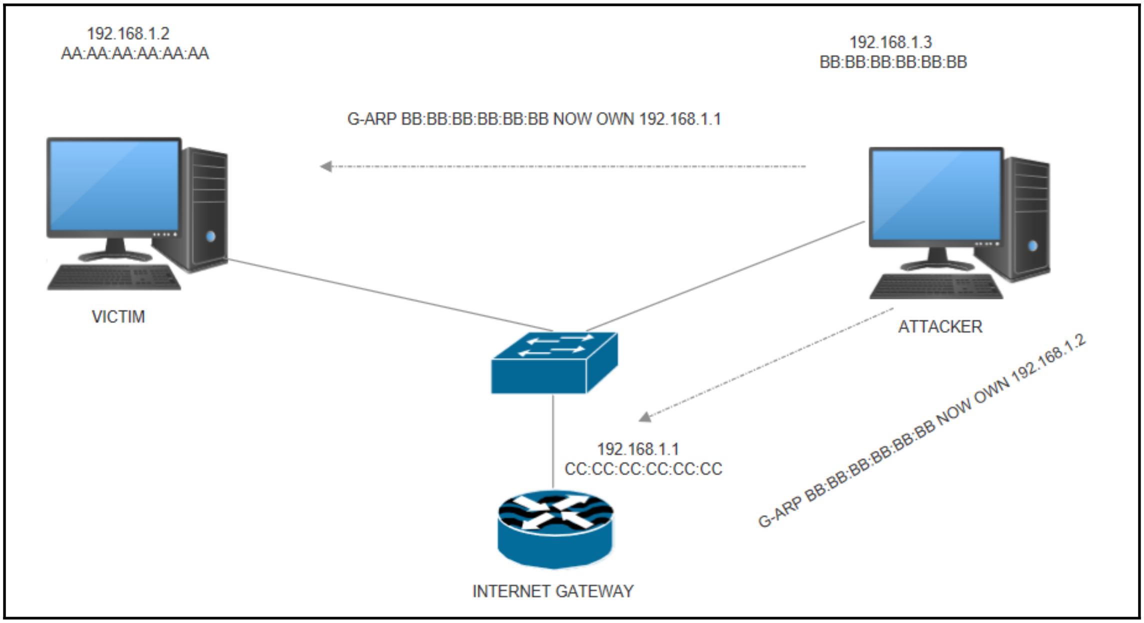


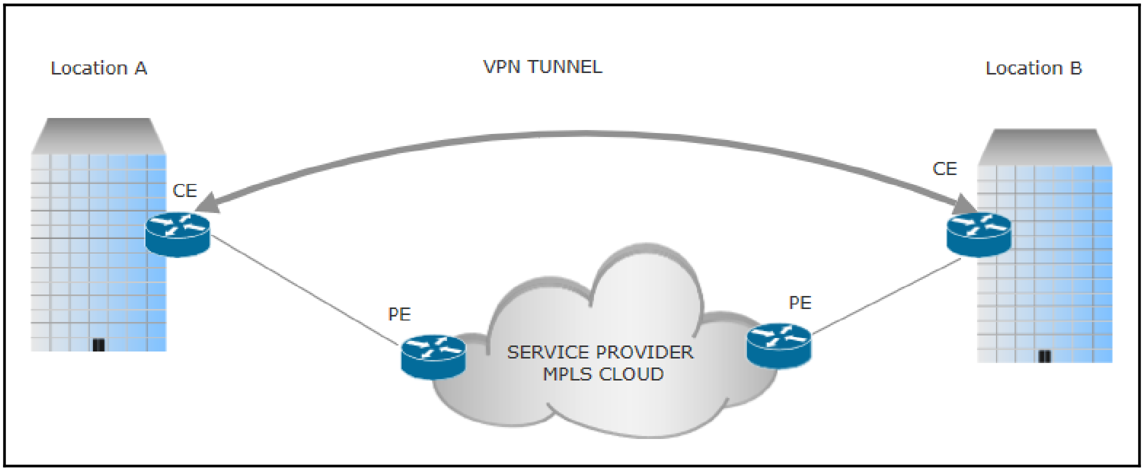
```
                          #show mac address-table count

Mac Entries for Vlan 201:
---------------------------
Dynamic Address Count  : 141
Static  Address Count  : 0
Total Mac Addresses    : 141

Mac Entries for Vlan 301:
---------------------------
Dynamic Address Count  : 21
Static  Address Count  : 0
Total Mac Addresses    : 21

Total Mac Address Space Available: 7877

                          #
```

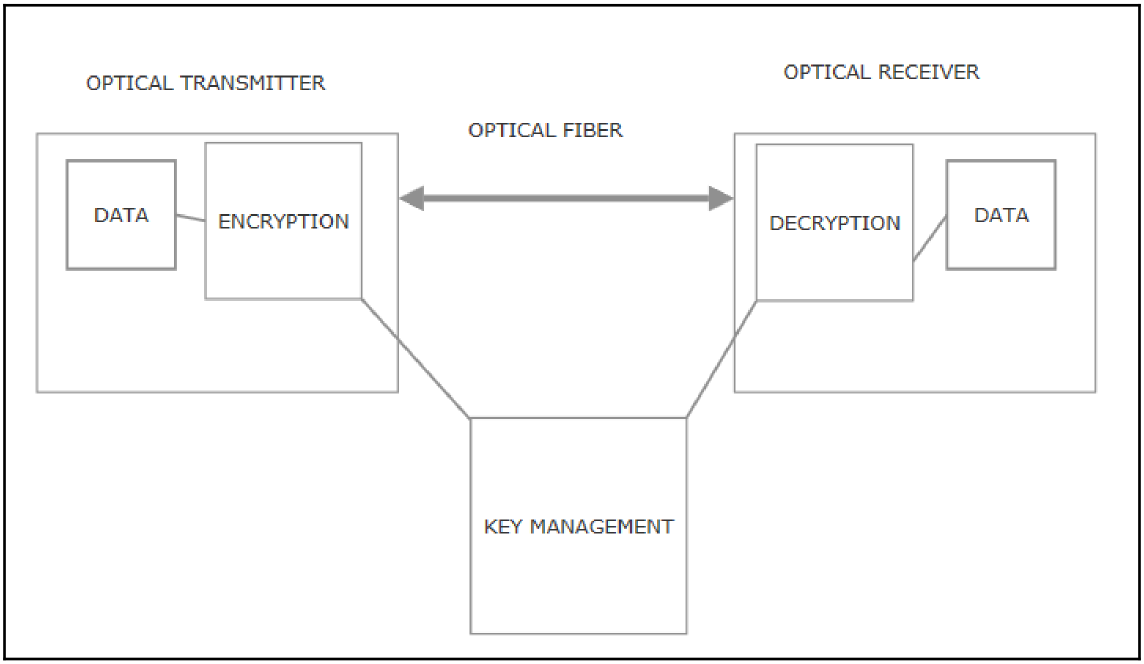


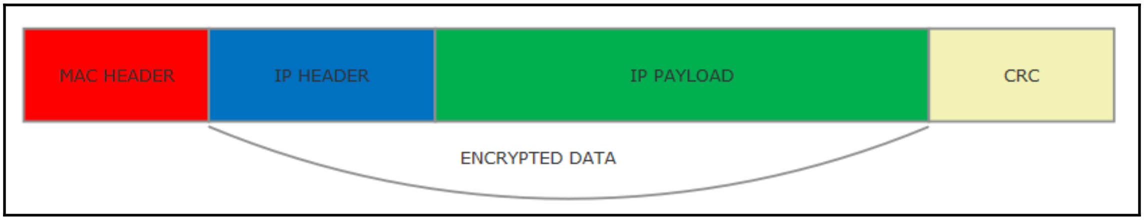
```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address 00D0.BC9A.42DC
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

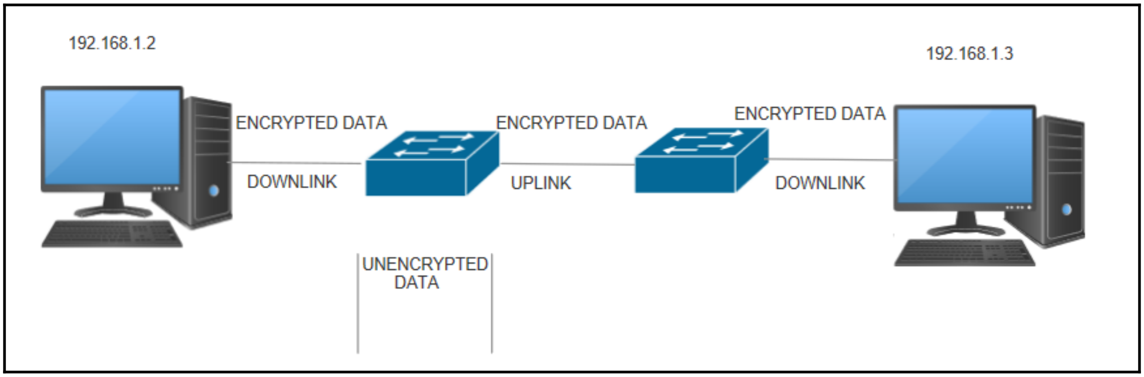

192.168.1.2
AA:AA:AA:AA:AA:AA
192.168.1.3
BB:BB:BB:BB:BB:BB
VICTIM
ARP REQUEST
WHO IS 192.168.1.1 ?
ATTACKER
ARP REPLY
MAC CC...CC
192.168.1.1
192.168.1.1
CC:CC:CC:CC:CC:CC
INTERNET GATEWAY

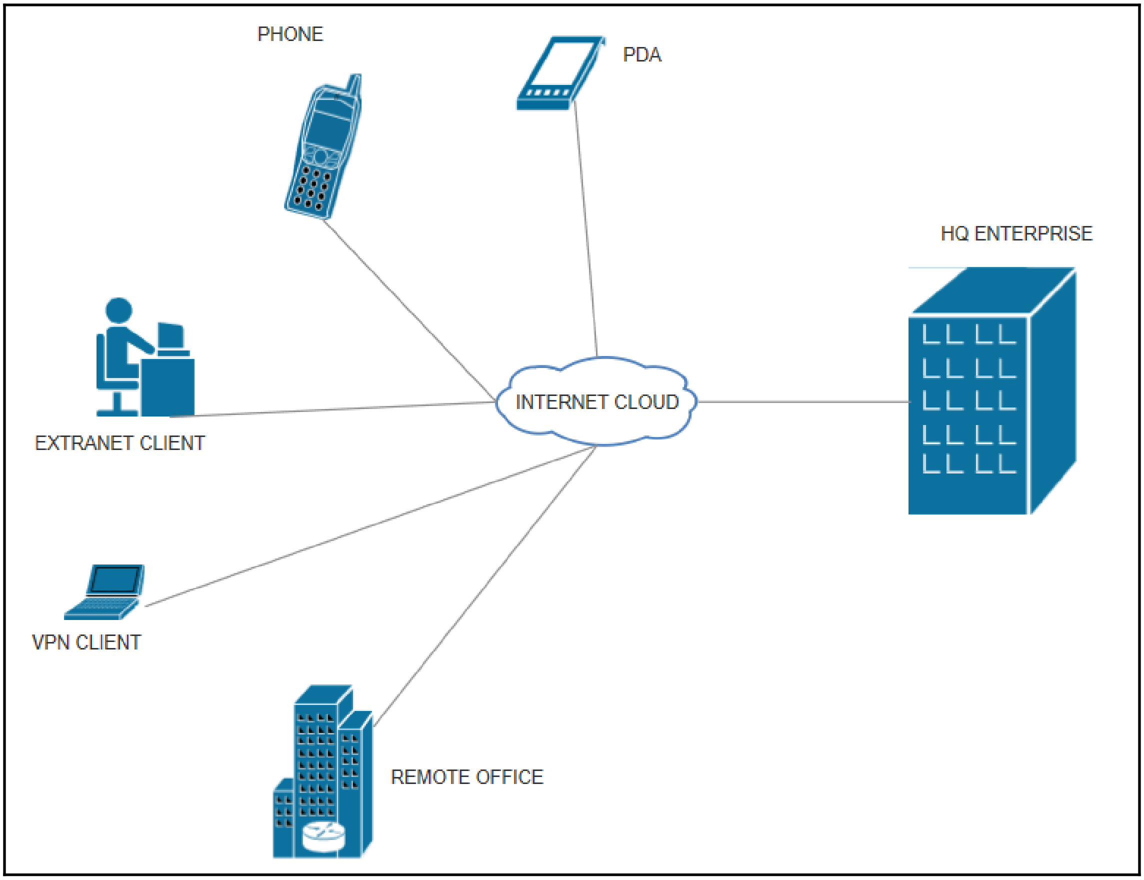

192.168.1.2
AA:AA:AA:AA:AA:AA
192.168.1.3
BB:BB:BB:BB:BB:BB
G-ARP BB:BB:BB:BB:BB:BB NOW OWN 192.168.1.1
VICTIM
ATTACKER
G-ARP BB:BB:BB:BB:BB:BB NOW OWN 192.168.1.2
192.168.1.1
CC:CC:CC:CC:CC:CC
INTERNET GATEWAY

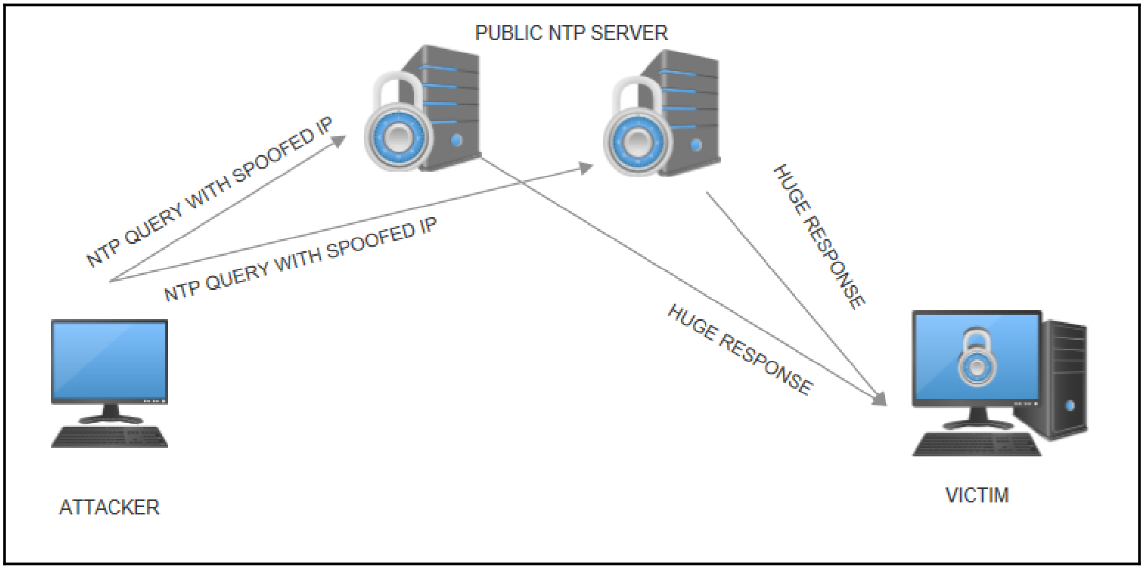

Location A
VPN TUNNEL
Location B
CE
CE
PE
PE
SERVICE PROVIDER
MPLS CLOUD

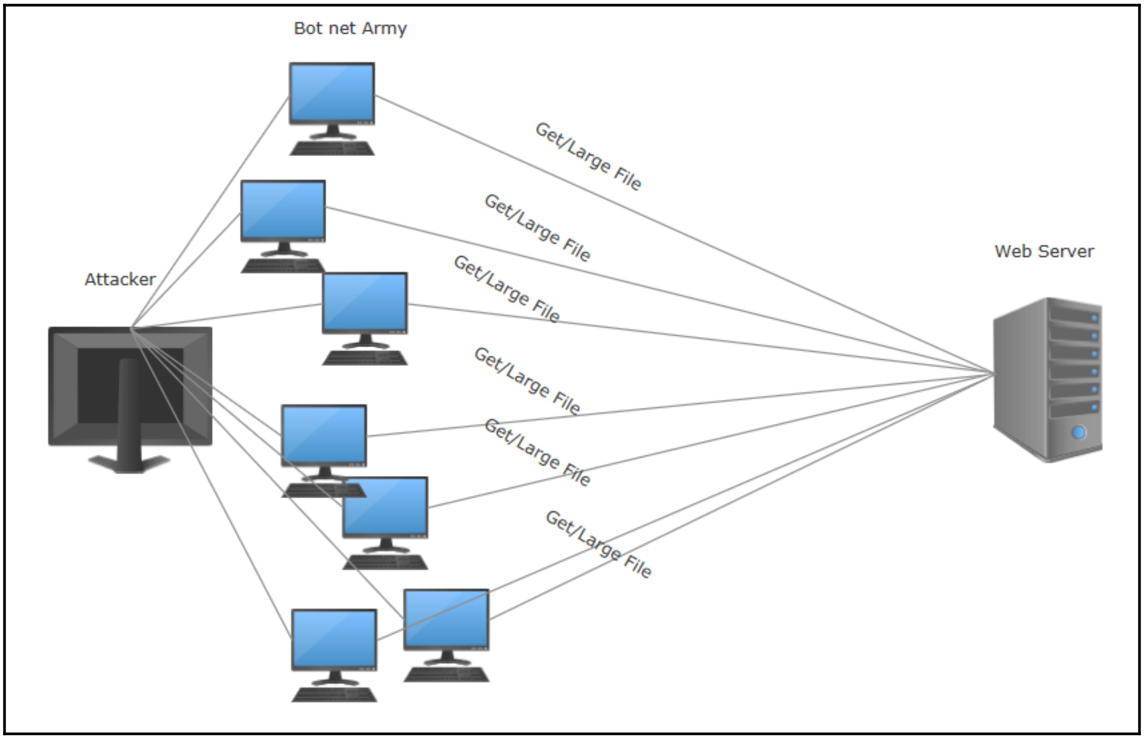

OPTICAL TRANSMITTER
OPTICAL RECEIVER
OPTICAL FIBER
DATA
ENCRYPTION
DECRYPTION
DATA
KEY MANAGEMENT

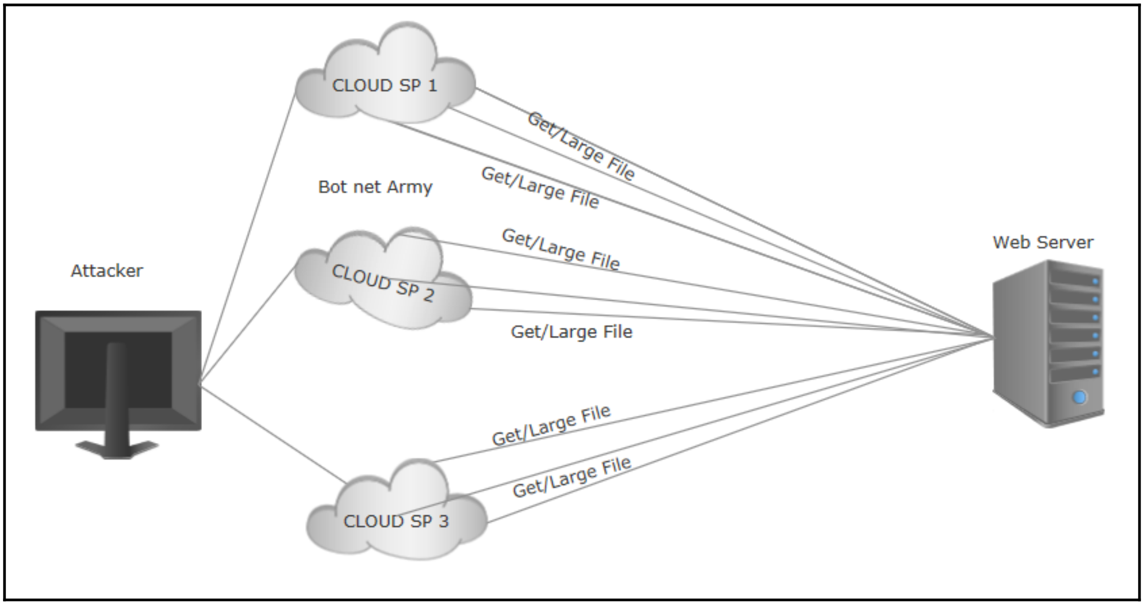

MAC HEADER
IP HEADER
IP PAYLOAD
CRC
ENCRYPTED DATA

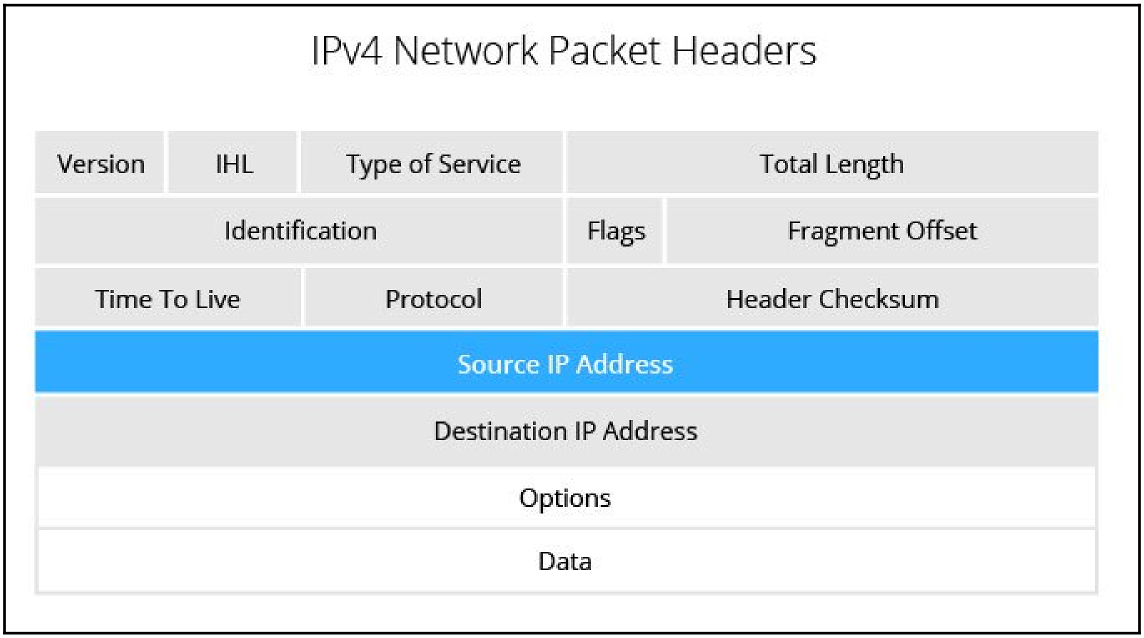

192.168.1.2
192.168.1.3
ENCRYPTED DATA
ENCRYPTED DATA
ENCRYPTED DATA
DOWNLINK
UPLINK
DOWNLINK
UNENCRYPTED DATA


PHONE
PDA
HQ ENTERPRISE
EXTRANET CLIENT
INTERNET CLOUD
VPN CLIENT
REMOTE OFFICE


PUBLIC NTP SERVER
NTP QUERY WITH SPOOFED IP
NTP QUERY WITH SPOOFED IP
HUGE RESPONSE
HUGE RESPONSE
ATTACKER
VICTIM

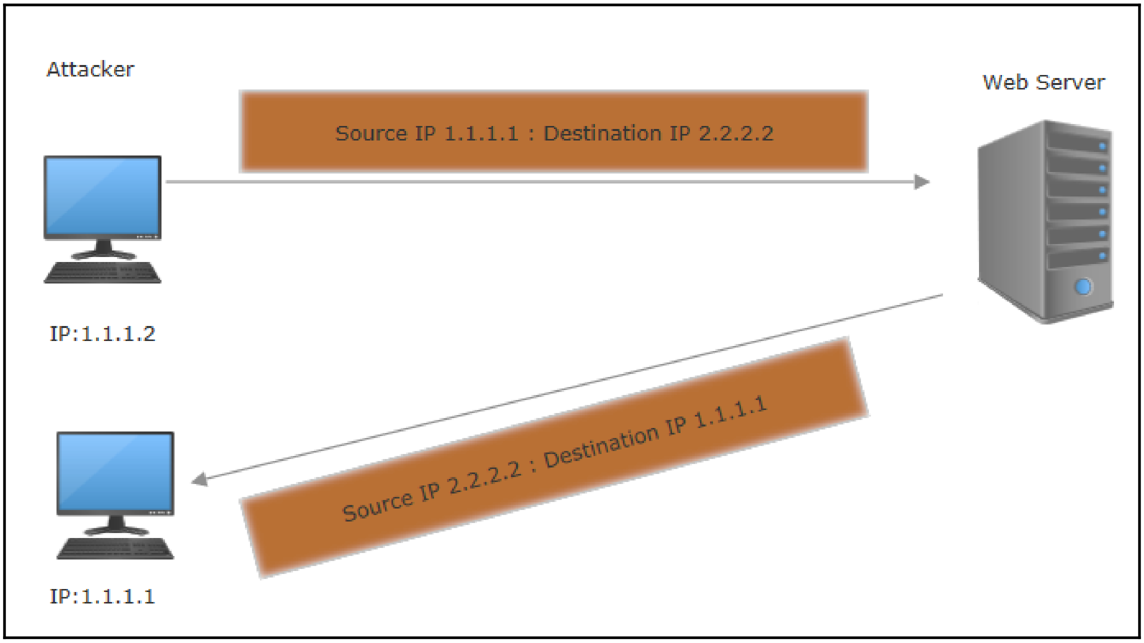

Bot net Army
Attacker
Web Server
Get/Large File
Get/Large File
Get/Large File
Get/Large File
Get/Large File
Get/Large File

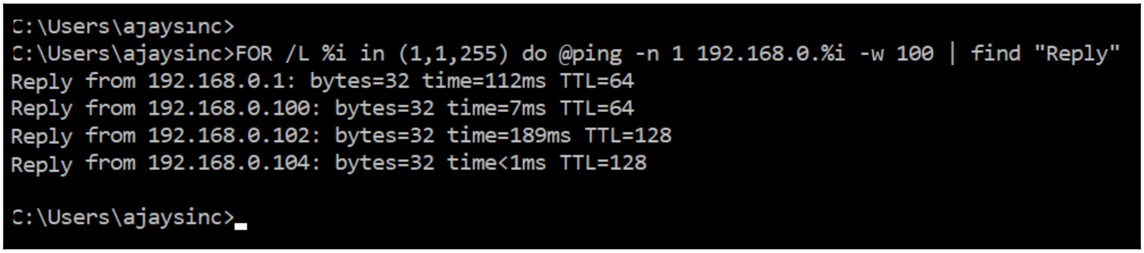




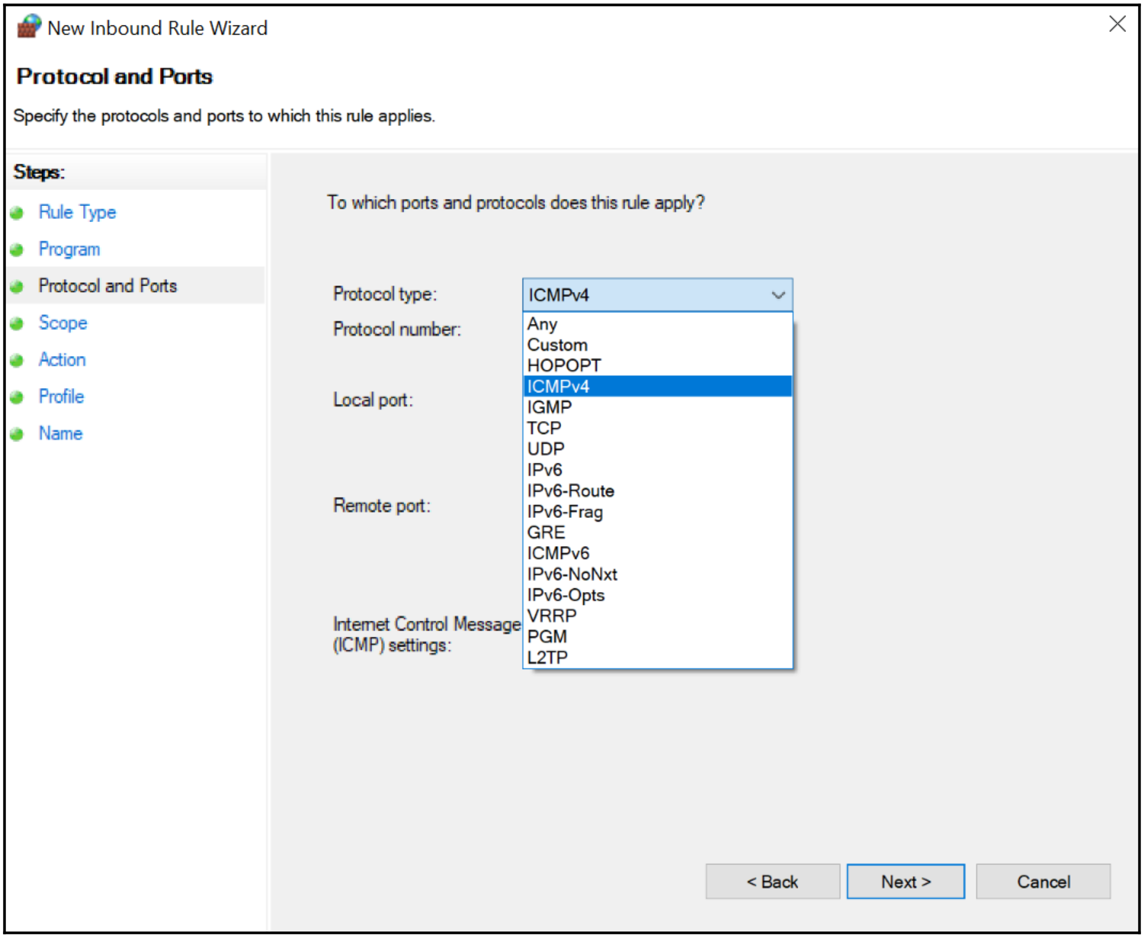
IPv4 Network Packet Headers

<table>
<tr><td>Version</td><td>IHL</td><td>Type of Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time To Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source IP Address</td></tr>
<tr><td colspan="5">Destination IP Address</td></tr>
<tr><td colspan="5">Options</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>


Attacker
Source IP 1.1.1.1 : Destination IP 2.2.2.2
Web Server
IP:1.1.1.2
Source IP 2.2.2.2 : Destination IP 1.1.1.1
IP:1.1.1.1



```
C:\Users\ajaysinc>
C:\Users\ajaysinc>FOR /L %i in (1,1,255) do @ping -n 1 192.168.0.%i -w 100 | find "Reply"
Reply from 192.168.0.1: bytes=32 time=112ms TTL=64
Reply from 192.168.0.100: bytes=32 time=7ms TTL=64
Reply from 192.168.0.102: bytes=32 time=189ms TTL=128
Reply from 192.168.0.104: bytes=32 time<1ms TTL=128

C:\Users\ajaysinc>_
```



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

To which ports and protocols does this rule apply?

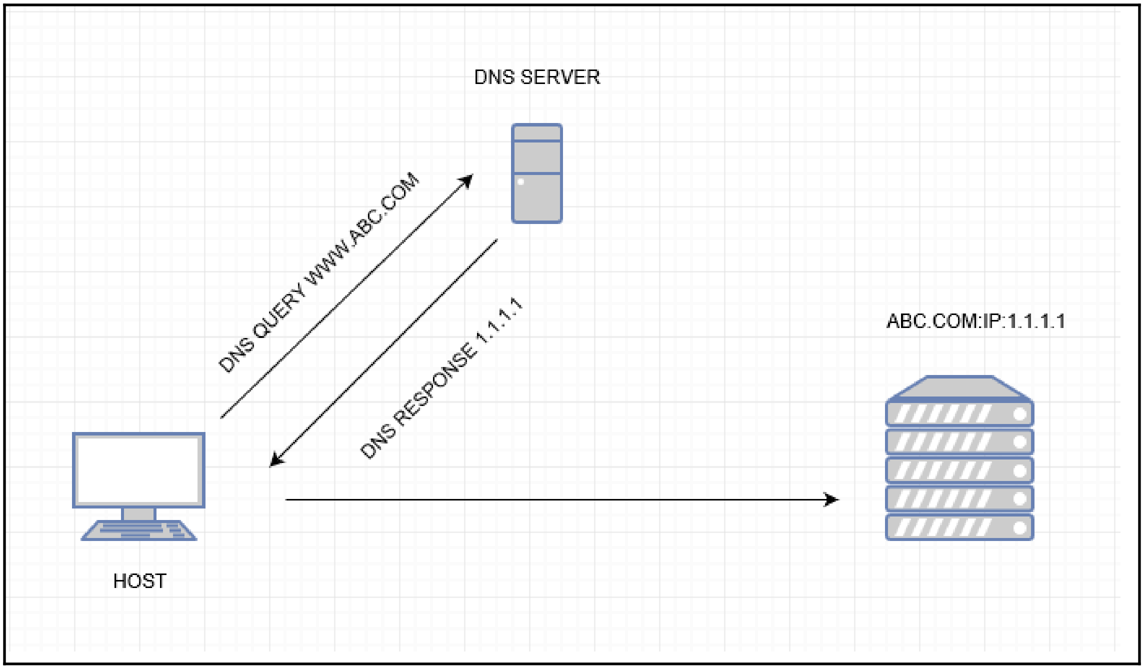
Protocol type: ICMPv4

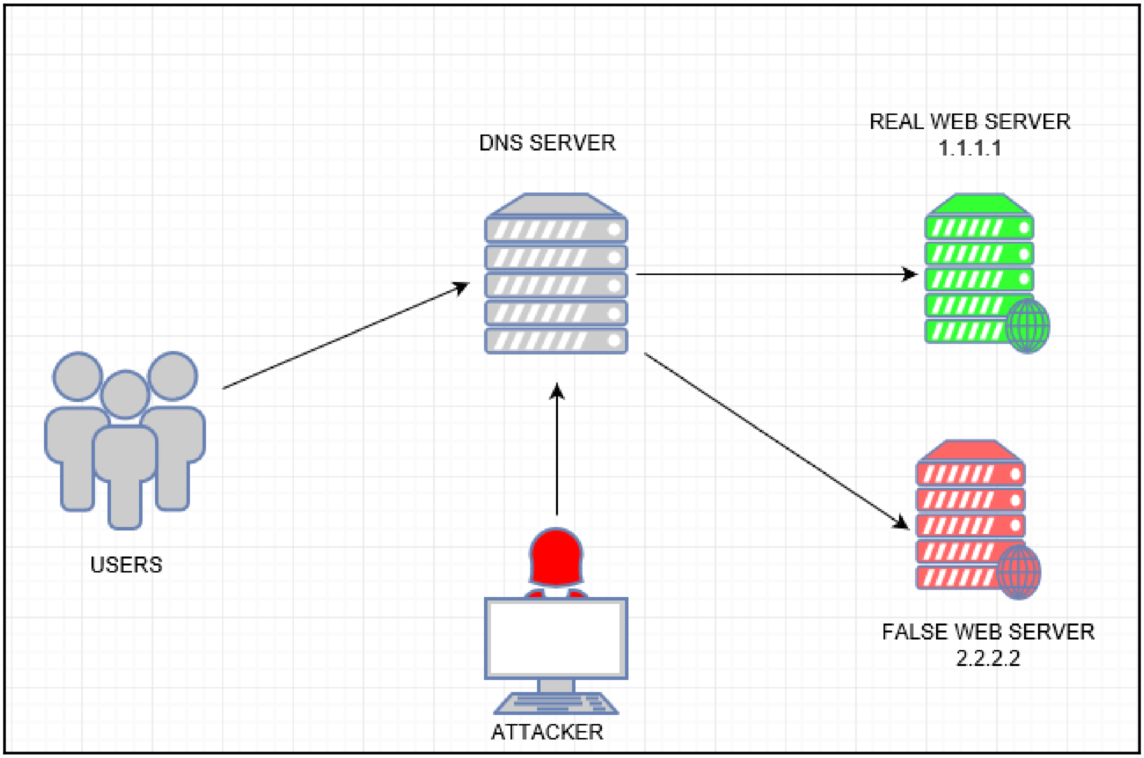
Protocol number:

Local port:

Remote port:

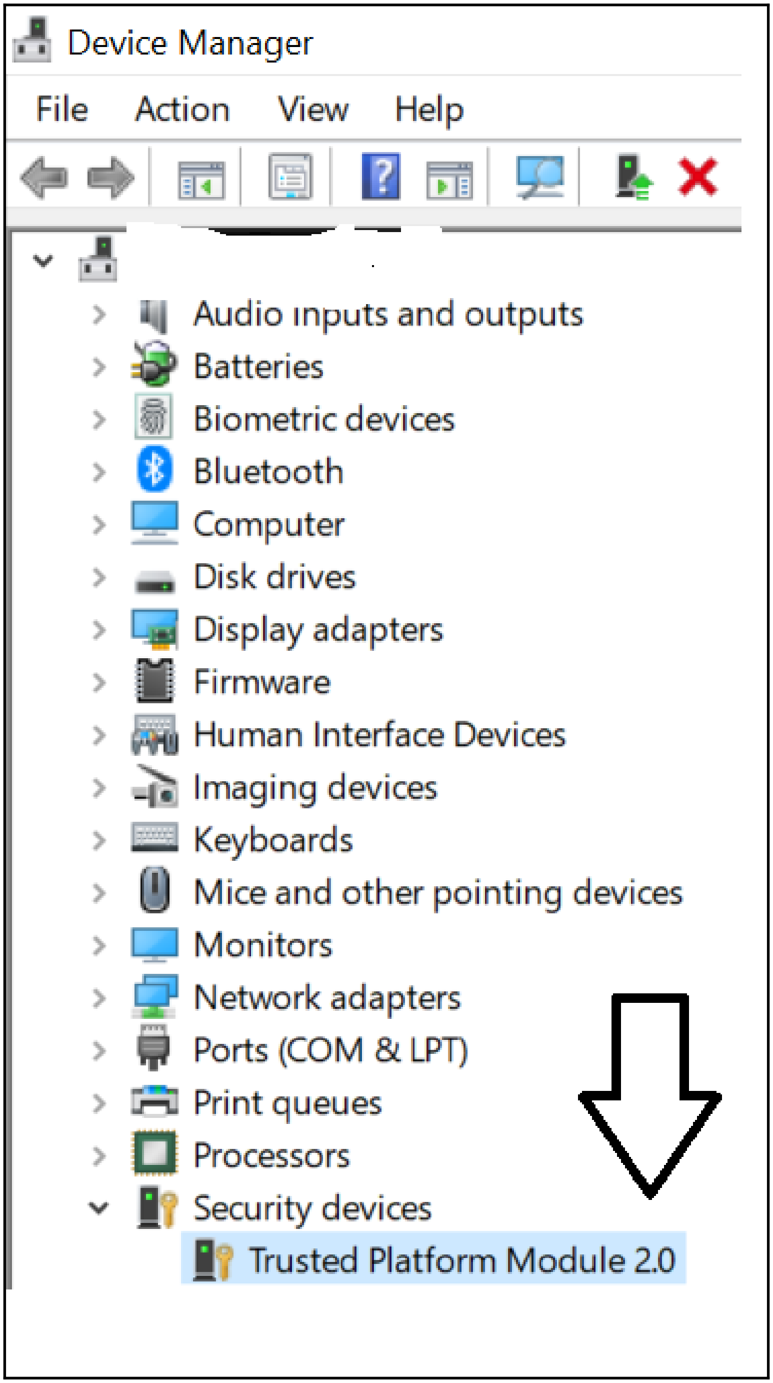
Internet Control Message (ICMP) settings:

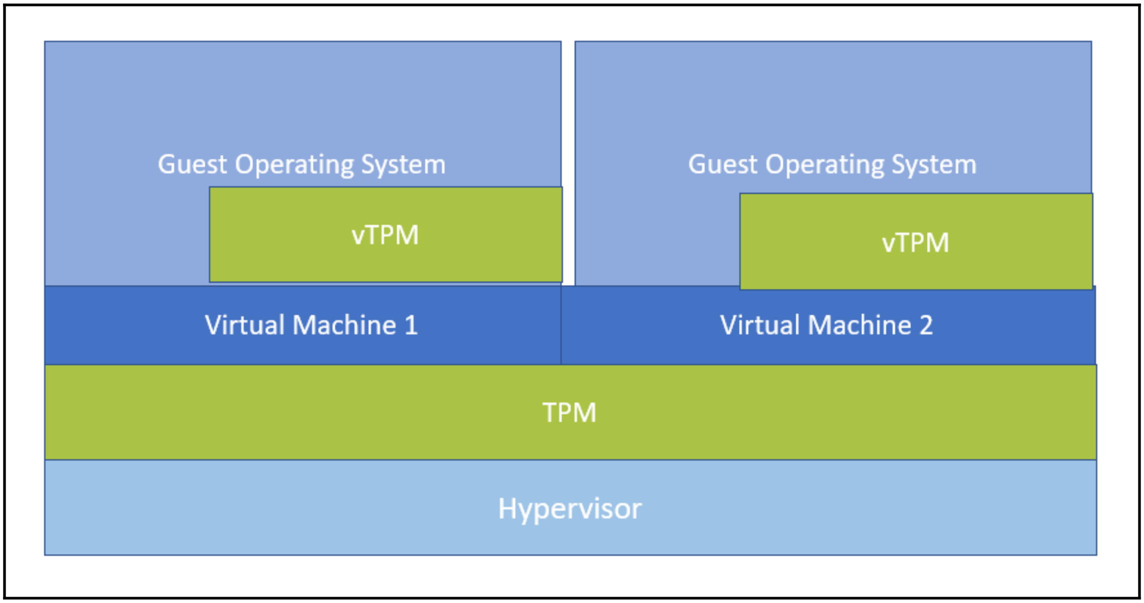

DNS SERVER
DNS QUERY WWW.ABC.COM
DNS RESPONSE 1.1.1.1
ABC.COM:IP:1.1.1.1
HOST

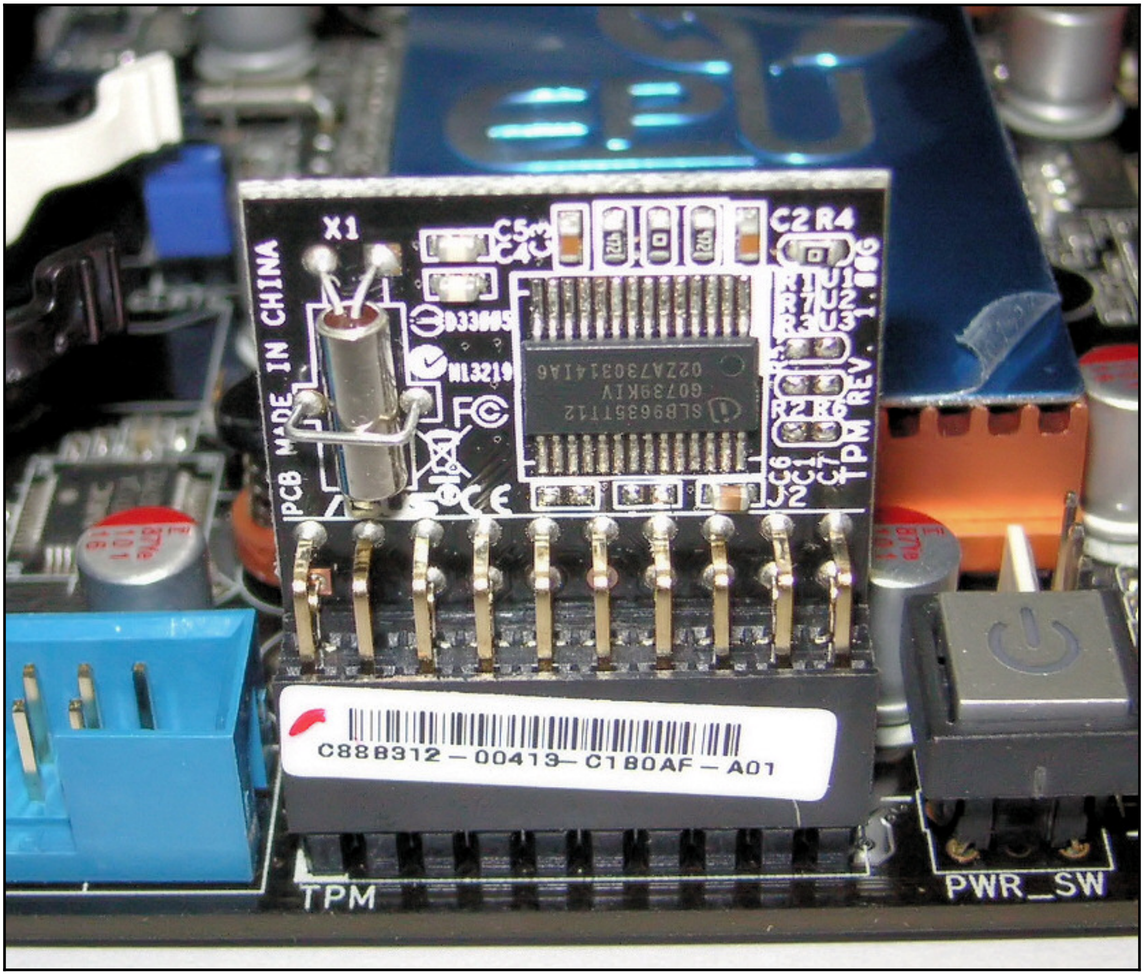

DNS SERVER
REAL WEB SERVER
1.1.1.1
USERS
FALSE WEB SERVER
2.2.2.2
ATTACKER

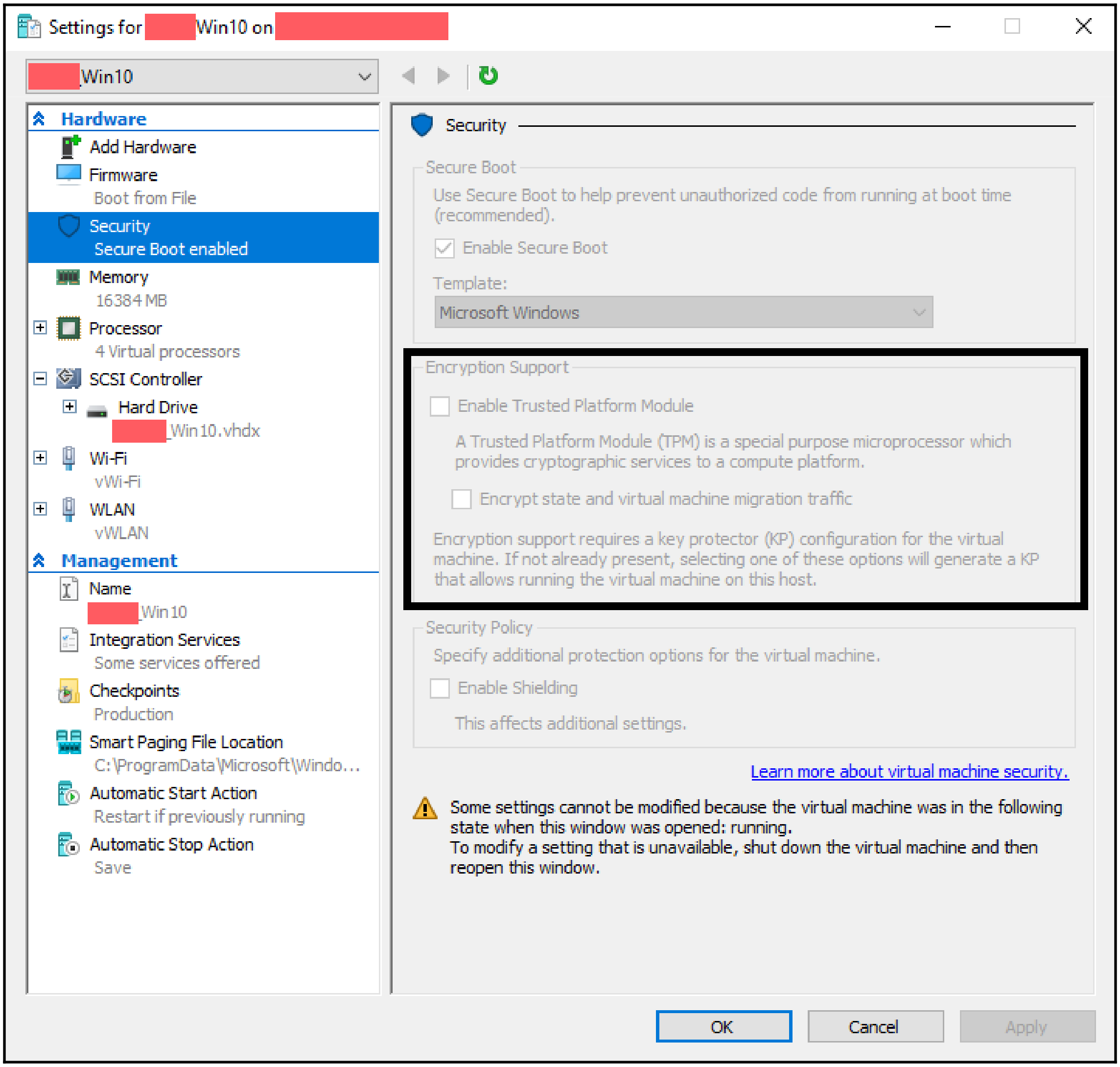
RSA
SecurID®
443 853
Secured by RSA

Chapter 3: Server level Security


Device Manager
File
Action
View
Help
Audio inputs and outputs
Batteries
Biometric devices
Bluetooth
Computer
Disk drives
Display adapters
Firmware
Human Interface Devices
Imaging devices
Keyboards
Mice and other pointing devices
Monitors
Network adapters
Ports (COM & LPT)
Print queues
Processors
Security devices
Trusted Platform Module 2.0


Guest Operating System
vTPM
Guest Operating System
vTPM
Virtual Machine 1
Virtual Machine 2
TPM
Hypervisor


X1
PCB MADE IN CHINA
C5
C4
C2 R4
R1 U1
R7 U2
R3 U3
R2 R6
TPM REV 1.00G
C6
C1
C7
J2
SLB9635TT12
G0739KIV
02ZA7303141A6
FC
CE
C88B312—00413—C180AF—A01
TPM
PWR_SW



Settings for [redacted] Win10 on [redacted]

[redacted] Win10

Hardware

Add Hardware

Firmware
Boot from File

Security
Secure Boot enabled

Memory
16384 MB

Processor
4 Virtual processors

SCSI Controller

Hard Drive
[redacted] Win10.vhdx

Wi-Fi
vWi-Fi

WLAN
vWLAN

Management

Name
[redacted] Win10

Integration Services
Some services offered

Checkpoints
Production

Smart Paging File Location
C:\ProgramData\Microsoft\Windo...

Automatic Start Action
Restart if previously running

Automatic Stop Action
Save

Security

Secure Boot

Use Secure Boot to help prevent unauthorized code from running at boot time (recommended).

☑ Enable Secure Boot

Template:
Microsoft Windows

Encryption Support

□ Enable Trusted Platform Module

A Trusted Platform Module (TPM) is a special purpose microprocessor which provides cryptographic services to a compute platform.

□ Encrypt state and virtual machine migration traffic

Encryption support requires a key protector (KP) configuration for the virtual machine. If not already present, selecting one of these options will generate a KP that allows running the virtual machine on this host.

Security Policy

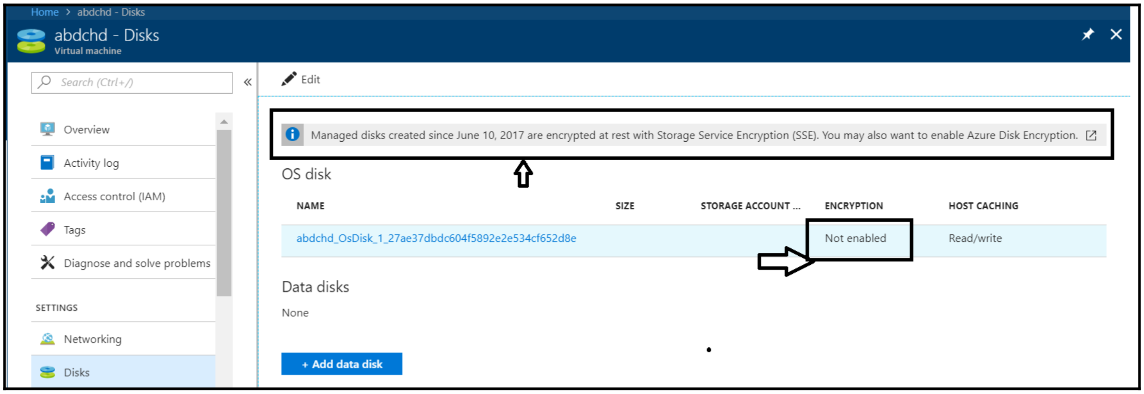
Specify additional protection options for the virtual machine.

□ Enable Shielding

This affects additional settings.

Learn more about virtual machine security.

Some settings cannot be modified because the virtual machine was in the following state when this window was opened: running.
To modify a setting that is unavailable, shut down the virtual machine and then reopen this window.



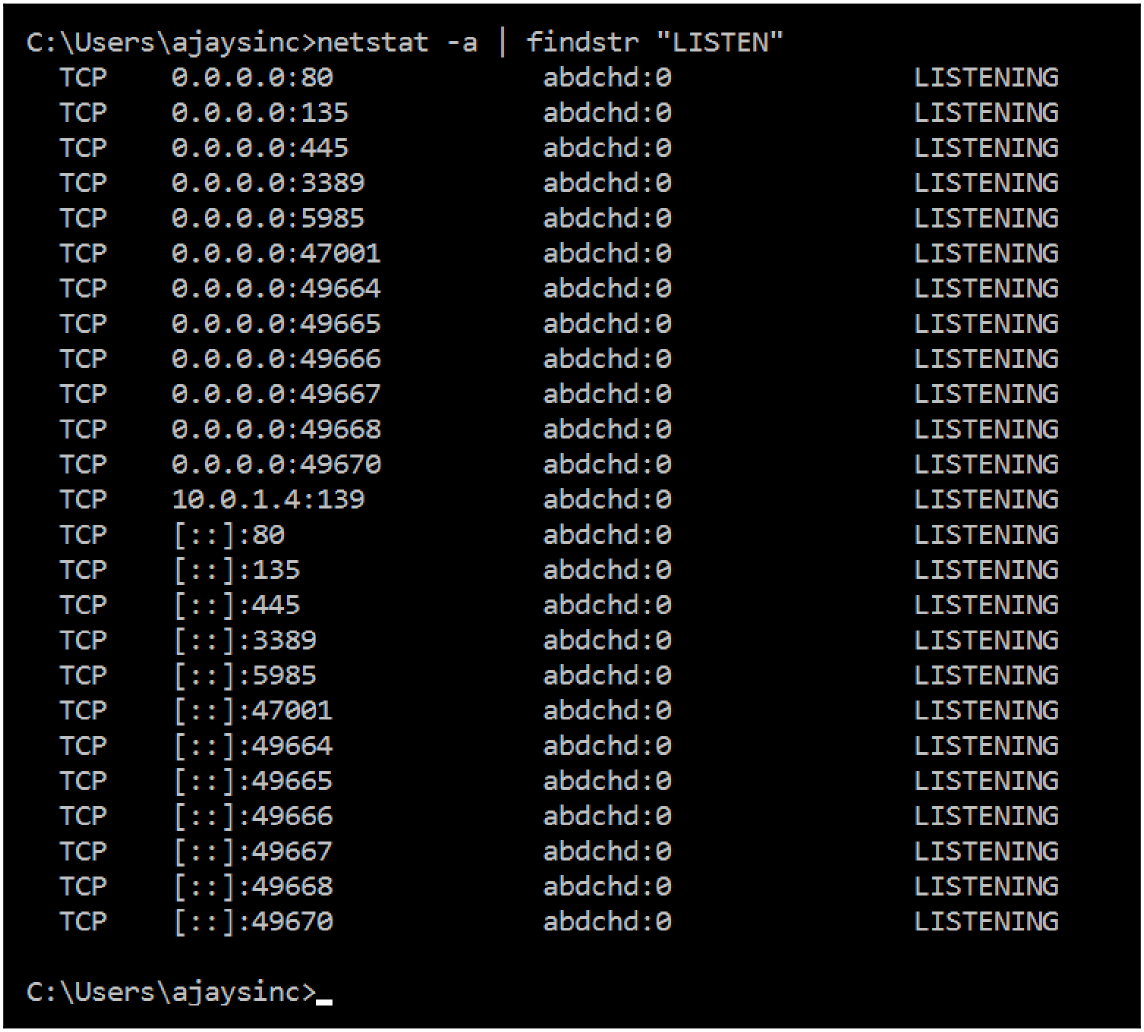
Managed disks created since June 10, 2017 are encrypted at rest with Storage Service Encryption (SSE). You may also want to enable Azure Disk Encryption.

OS disk

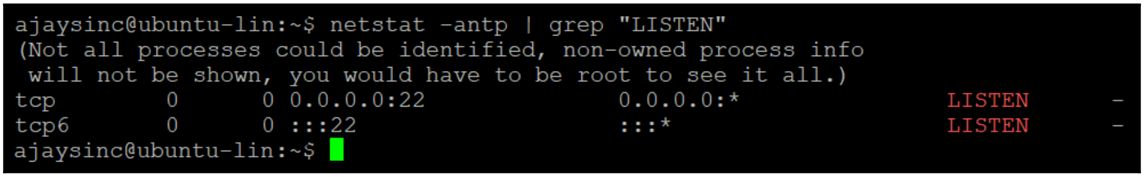
NAME	SIZE	STORAGE ACCOUNT ...	ENCRYPTION	HOST CACHING
abdchd_OsDisk_1_27ae37dbdc604f5892e2e534cf652d8e			Not enabled	Read/write

Data disks

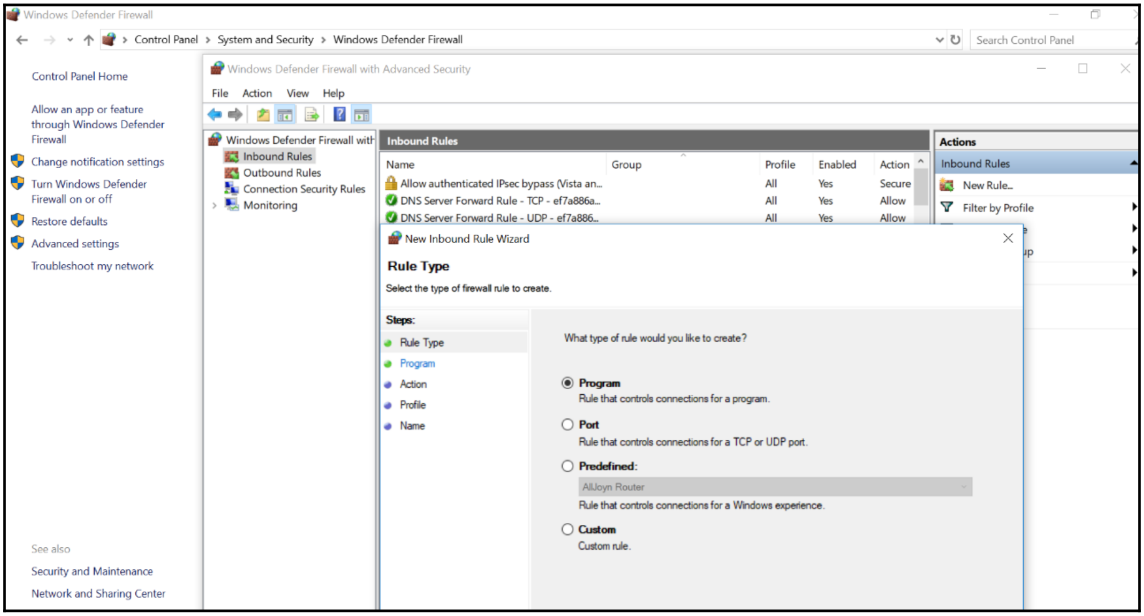
None



```
C:\Users\ajaysinc>netstat -a | findstr "LISTEN"
  TCP    0.0.0.0:80             abdchd:0               LISTENING
  TCP    0.0.0.0:135            abdchd:0               LISTENING
  TCP    0.0.0.0:445            abdchd:0               LISTENING
  TCP    0.0.0.0:3389           abdchd:0               LISTENING
  TCP    0.0.0.0:5985           abdchd:0               LISTENING
  TCP    0.0.0.0:47001          abdchd:0               LISTENING
  TCP    0.0.0.0:49664          abdchd:0               LISTENING
  TCP    0.0.0.0:49665          abdchd:0               LISTENING
  TCP    0.0.0.0:49666          abdchd:0               LISTENING
  TCP    0.0.0.0:49667          abdchd:0               LISTENING
  TCP    0.0.0.0:49668          abdchd:0               LISTENING
  TCP    0.0.0.0:49670          abdchd:0               LISTENING
  TCP    10.0.1.4:139           abdchd:0               LISTENING
  TCP    [::]:80                abdchd:0               LISTENING
  TCP    [::]:135               abdchd:0               LISTENING
  TCP    [::]:445               abdchd:0               LISTENING
  TCP    [::]:3389              abdchd:0               LISTENING
  TCP    [::]:5985              abdchd:0               LISTENING
  TCP    [::]:47001             abdchd:0               LISTENING
  TCP    [::]:49664             abdchd:0               LISTENING
  TCP    [::]:49665             abdchd:0               LISTENING
  TCP    [::]:49666             abdchd:0               LISTENING
  TCP    [::]:49667             abdchd:0               LISTENING
  TCP    [::]:49668             abdchd:0               LISTENING
  TCP    [::]:49670             abdchd:0               LISTENING

C:\Users\ajaysinc>_
```



```
ajaysinc@ubuntu-lin:~$ netstat -antp | grep "LISTEN"
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
ajaysinc@ubuntu-lin:~$
```


Windows Defender Firewall
Control Panel > System and Security > Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center
Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Actions
Inbound Rules
New Rule...
Filter by Profile

Inbound Rules

Name	Group	Profile	Enabled	Action
Allow authenticated IPsec bypass (Vista an...		All	Yes	Secure
DNS Server Forward Rule - TCP - ef7a886a...		All	Yes	Allow
DNS Server Forward Rule - UDP - ef7a886...		All	Yes	Allow

New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Program
- Action
- Profile
- Name

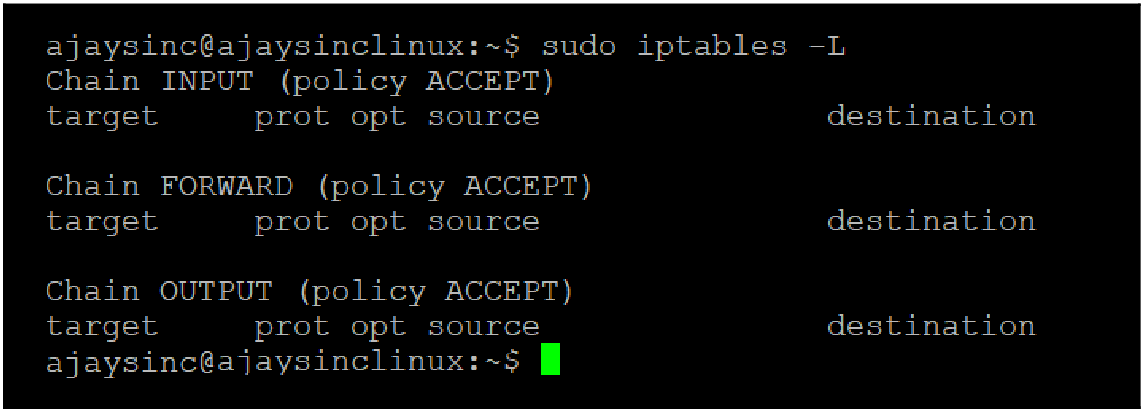
What type of rule would you like to create?

● **Program**
Rule that controls connections for a program.

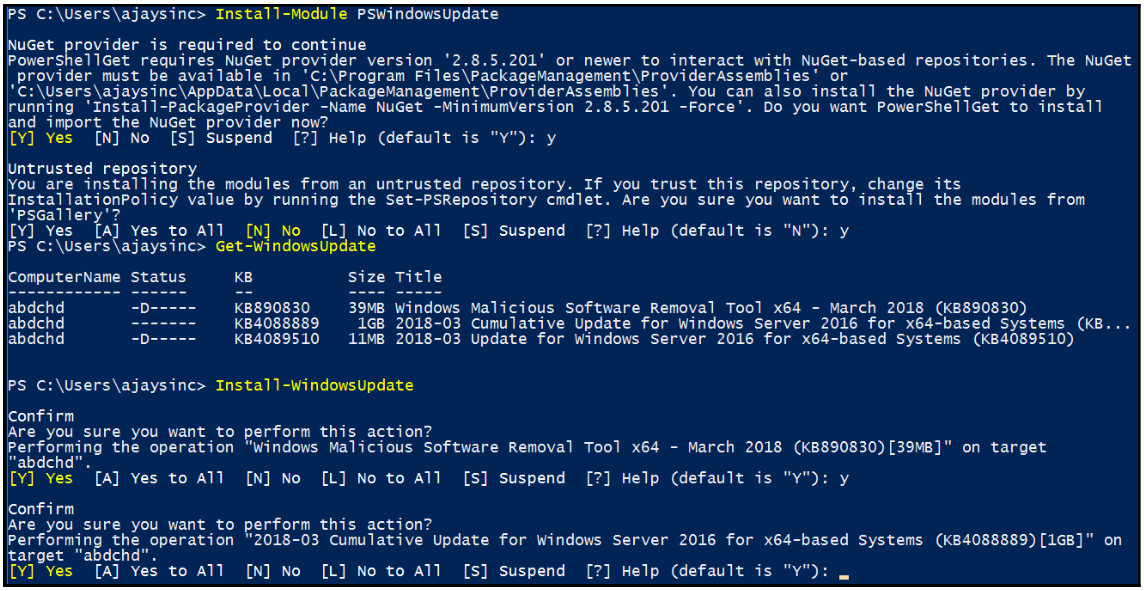
○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

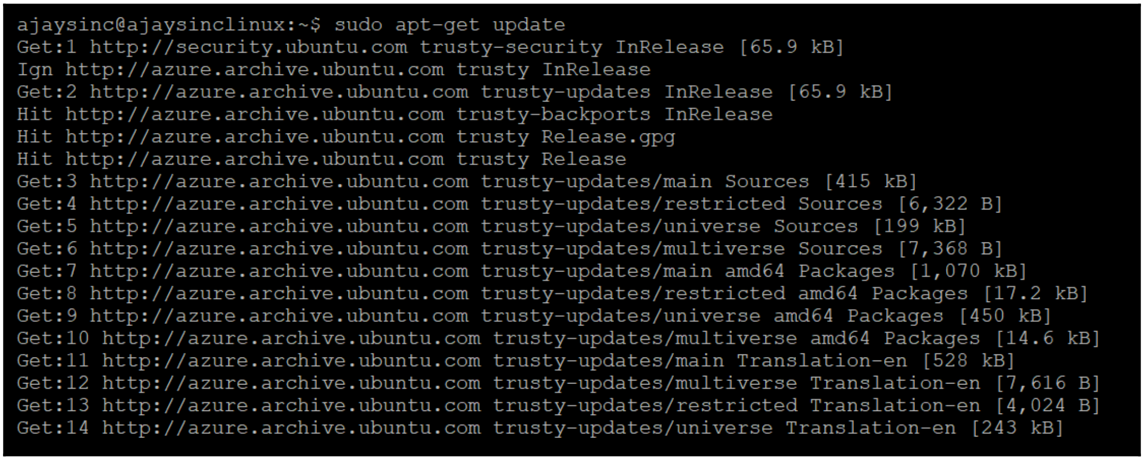
○ **Custom**
Custom rule.



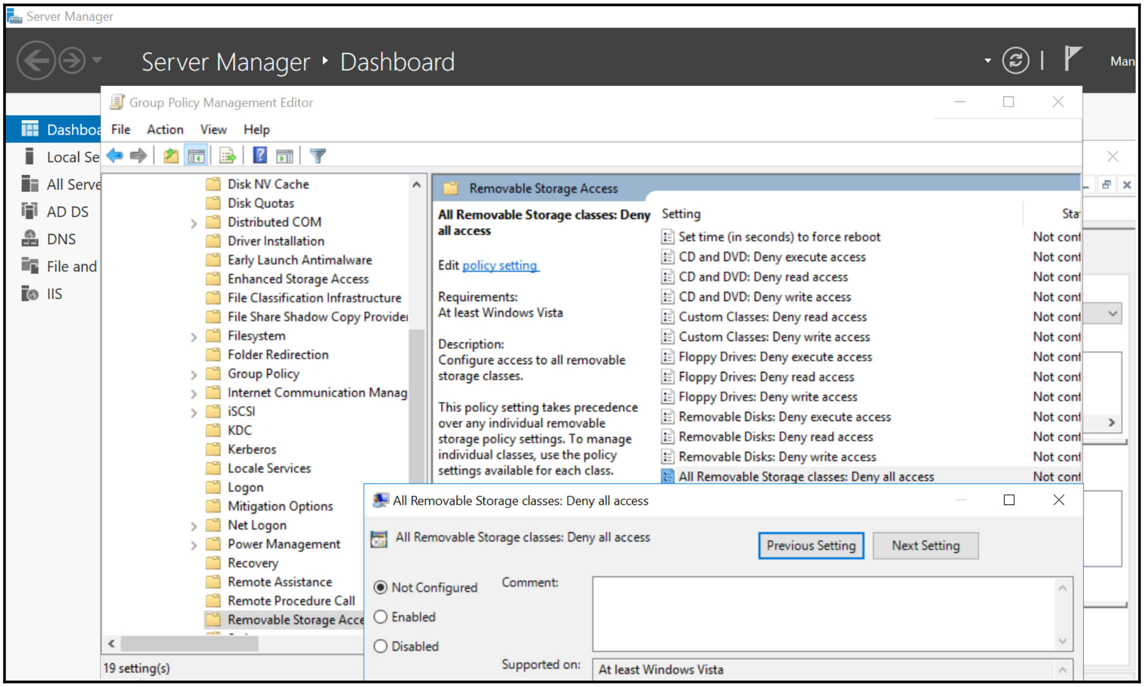
```
ajaysinc@ajaysinclinux:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ajaysinc@ajaysinclinux:~$
```



```
PS C:\Users\ajaysinc> Install-Module PSWindowsUpdate

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
 provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\ajaysinc\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install
and import the NuGet provider now?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): y
PS C:\Users\ajaysinc> Get-WindowsUpdate

ComputerName Status     KB          Size Title
------------ ------     --          ---- -----
abdchd       -D-----    KB890830    39MB Windows Malicious Software Removal Tool x64 - March 2018 (KB890830)
abdchd       -------    KB4088889    1GB 2018-03 Cumulative Update for Windows Server 2016 for x64-based Systems (KB...
abdchd       -D-----    KB4089510   11MB 2018-03 Update for Windows Server 2016 for x64-based Systems (KB4089510)


PS C:\Users\ajaysinc> Install-WindowsUpdate

Confirm
Are you sure you want to perform this action?
Performing the operation "Windows Malicious Software Removal Tool x64 - March 2018 (KB890830)[39MB]" on target
"abdchd".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Confirm
Are you sure you want to perform this action?
Performing the operation "2018-03 Cumulative Update for Windows Server 2016 for x64-based Systems (KB4088889)[1GB]" on
target "abdchd".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): _
```



```
ajaysinc@ajaysinclinux:~$ sudo apt-get update
Get:1 http://security.ubuntu.com trusty-security InRelease [65.9 kB]
Ign http://azure.archive.ubuntu.com trusty InRelease
Get:2 http://azure.archive.ubuntu.com trusty-updates InRelease [65.9 kB]
Hit http://azure.archive.ubuntu.com trusty-backports InRelease
Hit http://azure.archive.ubuntu.com trusty Release.gpg
Hit http://azure.archive.ubuntu.com trusty Release
Get:3 http://azure.archive.ubuntu.com trusty-updates/main Sources [415 kB]
Get:4 http://azure.archive.ubuntu.com trusty-updates/restricted Sources [6,322 B]
Get:5 http://azure.archive.ubuntu.com trusty-updates/universe Sources [199 kB]
Get:6 http://azure.archive.ubuntu.com trusty-updates/multiverse Sources [7,368 B]
Get:7 http://azure.archive.ubuntu.com trusty-updates/main amd64 Packages [1,070 kB]
Get:8 http://azure.archive.ubuntu.com trusty-updates/restricted amd64 Packages [17.2 kB]
Get:9 http://azure.archive.ubuntu.com trusty-updates/universe amd64 Packages [450 kB]
Get:10 http://azure.archive.ubuntu.com trusty-updates/multiverse amd64 Packages [14.6 kB]
Get:11 http://azure.archive.ubuntu.com trusty-updates/main Translation-en [528 kB]
Get:12 http://azure.archive.ubuntu.com trusty-updates/multiverse Translation-en [7,616 B]
Get:13 http://azure.archive.ubuntu.com trusty-updates/restricted Translation-en [4,024 B]
Get:14 http://azure.archive.ubuntu.com trusty-updates/universe Translation-en [243 kB]
```



All Removable Storage classes: Deny all access

Edit policy setting

Requirements:
At least Windows Vista

Description:
Configure access to all removable storage classes.

This policy setting takes precedence over any individual removable storage policy settings. To manage individual classes, use the policy settings available for each class.

Setting	Sta
Set time (in seconds) to force reboot	Not conf
CD and DVD: Deny execute access	Not conf
CD and DVD: Deny read access	Not conf
CD and DVD: Deny write access	Not conf
Custom Classes: Deny read access	Not conf
Custom Classes: Deny write access	Not conf
Floppy Drives: Deny execute access	Not conf
Floppy Drives: Deny read access	Not conf
Floppy Drives: Deny write access	Not conf
Removable Disks: Deny execute access	Not conf
Removable Disks: Deny read access	Not conf
Removable Disks: Deny write access	Not conf
All Removable Storage classes: Deny all access	Not conf

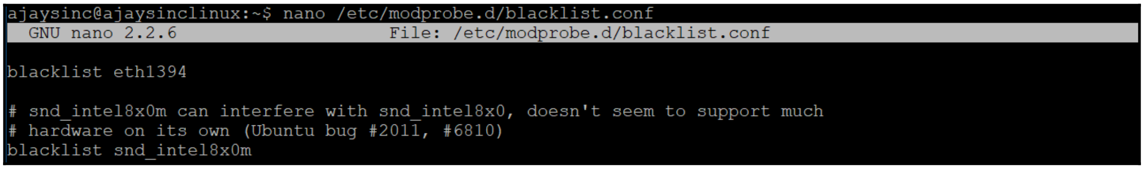
All Removable Storage classes: Deny all access

All Removable Storage classes: Deny all access

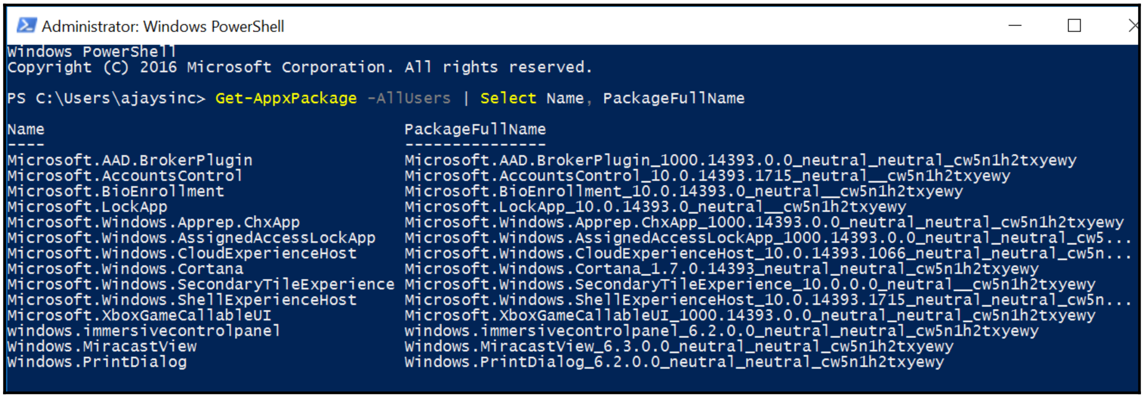
● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

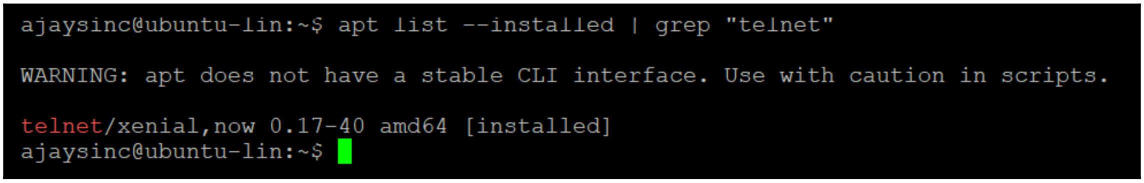


```
ajaysinc@ajaysinclinux:~$ nano /etc/modprobe.d/blacklist.conf
  GNU nano 2.2.6                  File: /etc/modprobe.d/blacklist.conf

blacklist eth1394

# snd_intel8x0m can interfere with snd_intel8x0, doesn't seem to support much
# hardware on its own (Ubuntu bug #2011, #6810)
blacklist snd_intel8x0m
```

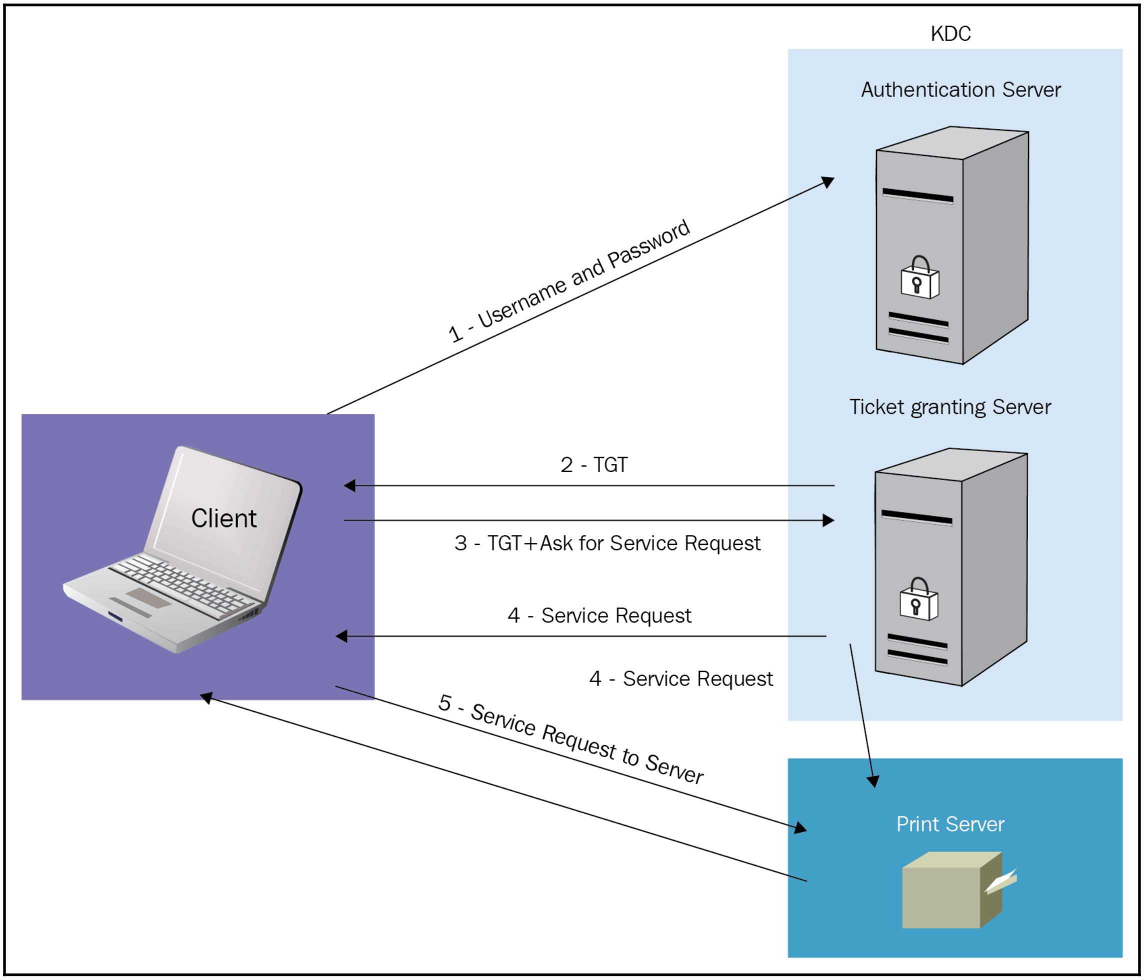


Administrator: Windows PowerShell

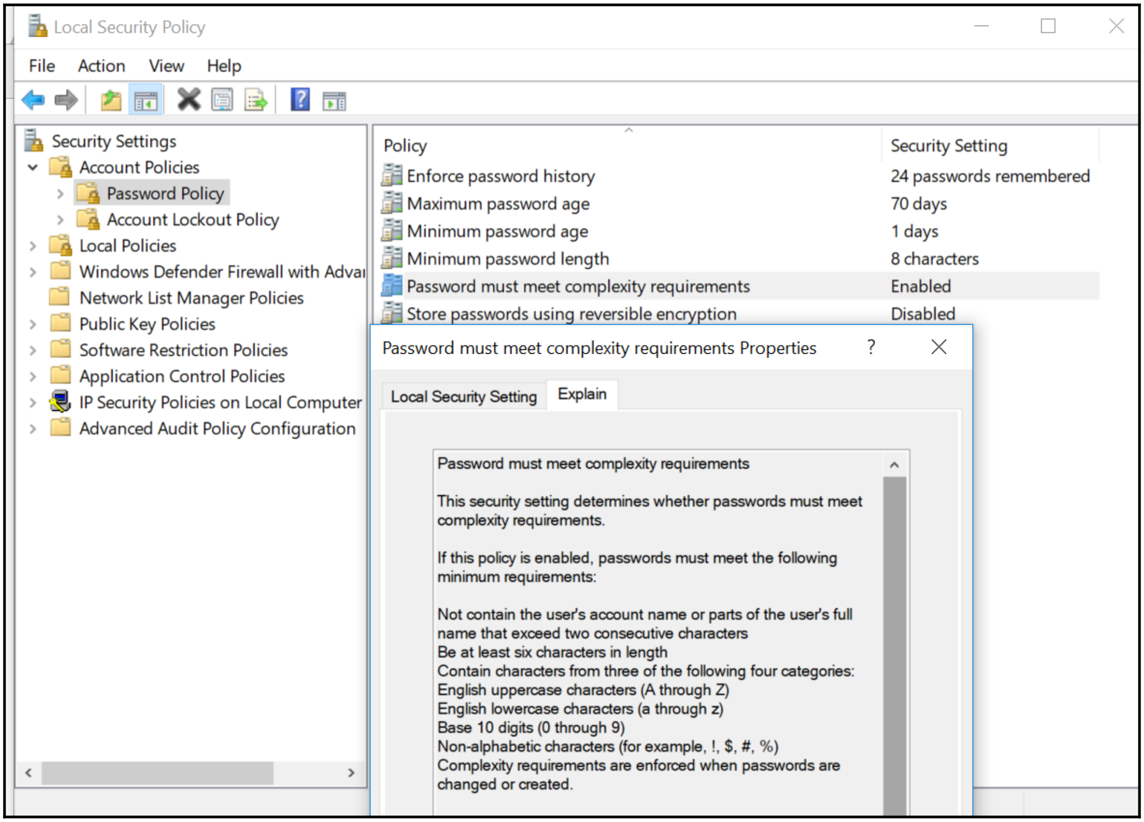
```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\ajaysinc> Get-AppxPackage -AllUsers | Select Name, PackageFullName

Name                                      PackageFullName
----                                      ---------------
Microsoft.AAD.BrokerPlugin                Microsoft.AAD.BrokerPlugin_1000.14393.0.0_neutral_neutral_cw5n1h2txyewy
Microsoft.AccountsControl                 Microsoft.AccountsControl_10.0.14393.1715_neutral__cw5n1h2txyewy
Microsoft.BioEnrollment                   Microsoft.BioEnrollment_10.0.14393.0_neutral__cw5n1h2txyewy
Microsoft.LockApp                         Microsoft.LockApp_10.0.14393.0_neutral__cw5n1h2txyewy
Microsoft.Windows.Apprep.ChxApp           Microsoft.Windows.Apprep.ChxApp_1000.14393.0.0_neutral_neutral_cw5n1h2txyewy
Microsoft.Windows.AssignedAccessLockApp   Microsoft.Windows.AssignedAccessLockApp_1000.14393.0.0_neutral_neutral_cw5...
Microsoft.Windows.CloudExperienceHost     Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_neutral_cw5n...
Microsoft.Windows.Cortana                 Microsoft.Windows.Cortana_1.7.0.14393_neutral_neutral_cw5n1h2txyewy
Microsoft.Windows.SecondaryTileExperience Microsoft.Windows.SecondaryTileExperience_10.0.0.0_neutral__cw5n1h2txyewy
Microsoft.Windows.ShellExperienceHost     Microsoft.Windows.ShellExperienceHost_10.0.14393.1715_neutral_neutral_cw5n...
Microsoft.XboxGameCallableUI              Microsoft.XboxGameCallableUI_1000.14393.0.0_neutral_neutral_cw5n1h2txyewy
windows.immersivecontrolpanel             windows.immersivecontrolpanel_6.2.0.0_neutral_neutral_cw5n1h2txyewy
Windows.MiracastView                      Windows.MiracastView_6.3.0.0_neutral_neutral_cw5n1h2txyewy
Windows.PrintDialog                       Windows.PrintDialog_6.2.0.0_neutral_neutral_cw5n1h2txyewy
```



```
ajaysinc@ubuntu-lin:~$ apt list --installed | grep "telnet"

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

telnet/xenial,now 0.17-40 amd64 [installed]
ajaysinc@ubuntu-lin:~$ 
```



NTLM	**Kerberos**
Challenge-Response based authentication	Ticket based authentication
Microsoft proprietary protocol	Open Standard protocol
The server connects the domain controller [DC] to validate the client's response for the challenge (known as pass-through authentication)	The client contacts the DC to get service ticket.
Due to Pass-through authentication for each session and DC is contacted each Time you access the services, which makes it more chatty.	Faster! The client manages a Tickets cache. No need to contact the DC for additional sessions to the same service if the ticket is still Valid.
Weak cryptographic and easy to crack	Strong cryptography


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Advai
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Password must meet complexity requirements Properties
?
Local Security Setting
Explain

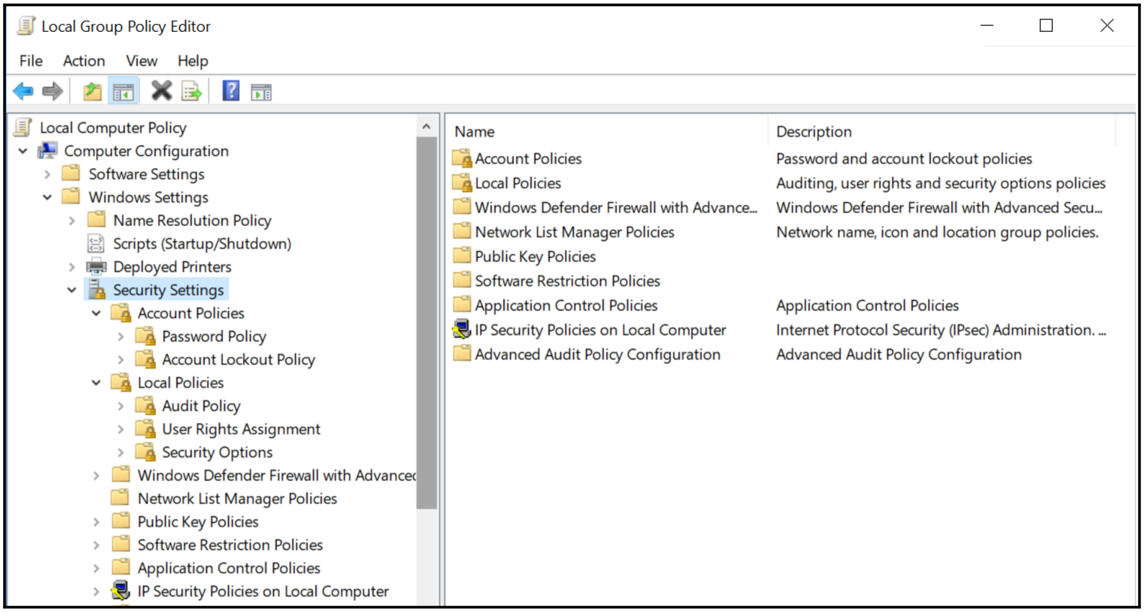
Policy	Security Setting
Enforce password history	24 passwords remembered
Maximum password age	70 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Password must meet complexity requirements

This security setting determines whether passwords must meet complexity requirements.

If this policy is enabled, passwords must meet the following minimum requirements:

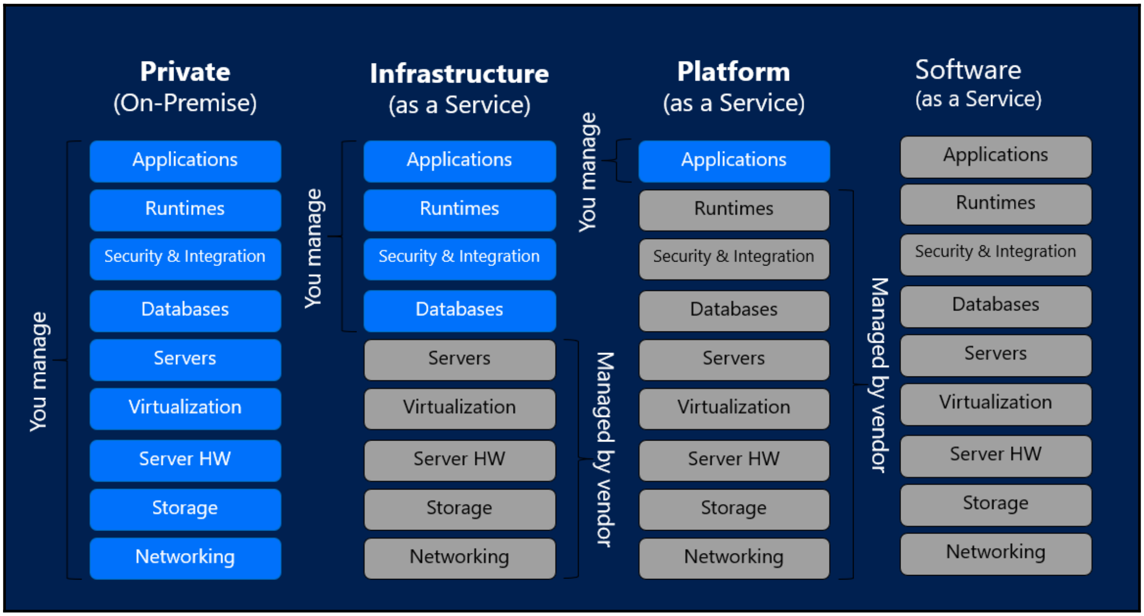
Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
Be at least six characters in length
Contain characters from three of the following four categories:
English uppercase characters (A through Z)
English lowercase characters (a through z)
Base 10 digits (0 through 9)
Non-alphabetic characters (for example, !, $, #, %)
Complexity requirements are enforced when passwords are changed or created.



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
          - Password Policy
          - Account Lockout Policy
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Windows Defender Firewall with Advancec
        - Network List Manager Policies
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Local Computer

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options policies
Windows Defender Firewall with Advance...	Windows Defender Firewall with Advanced Secu...
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administration. ...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

Chapter 4: Cloud Security Design



Private
(On-Premise)

You manage

- Applications
- Runtimes
- Security & Integration
- Databases
- Servers
- Virtualization
- Server HW
- Storage
- Networking

Infrastructure
(as a Service)

You manage

- Applications
- Runtimes
- Security & Integration
- Databases

Managed by vendor

- Servers
- Virtualization
- Server HW
- Storage
- Networking

Platform
(as a Service)

You manage

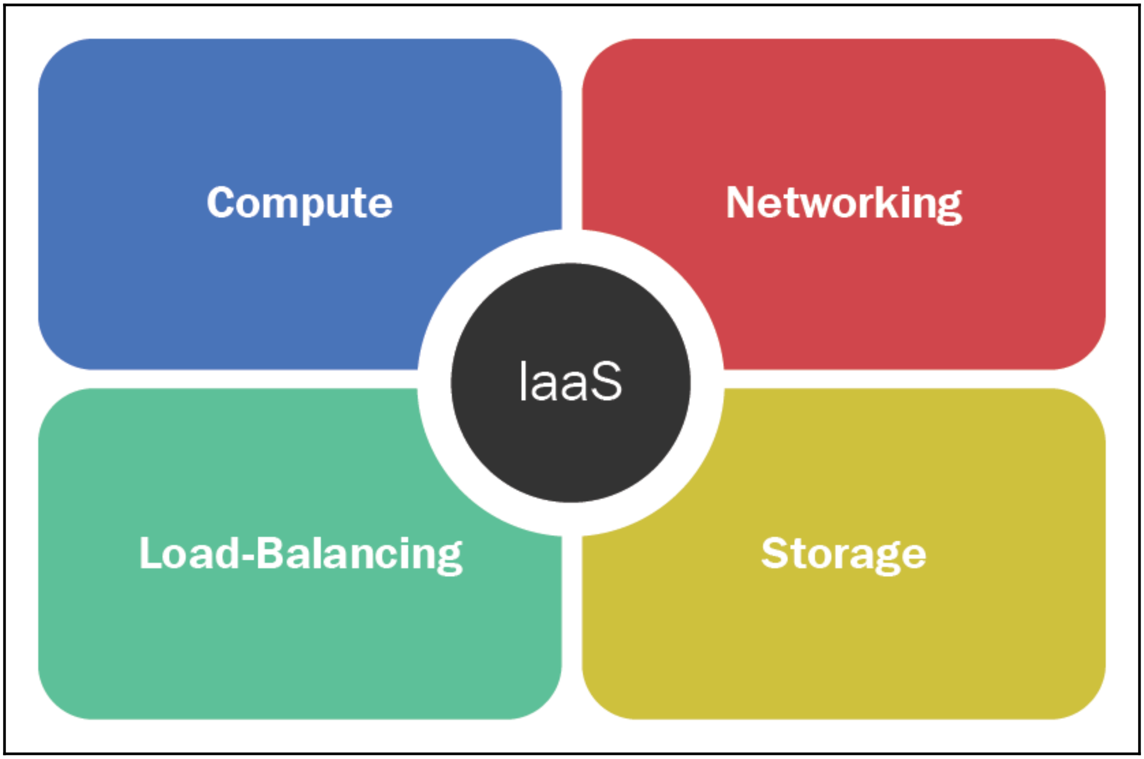
- Applications

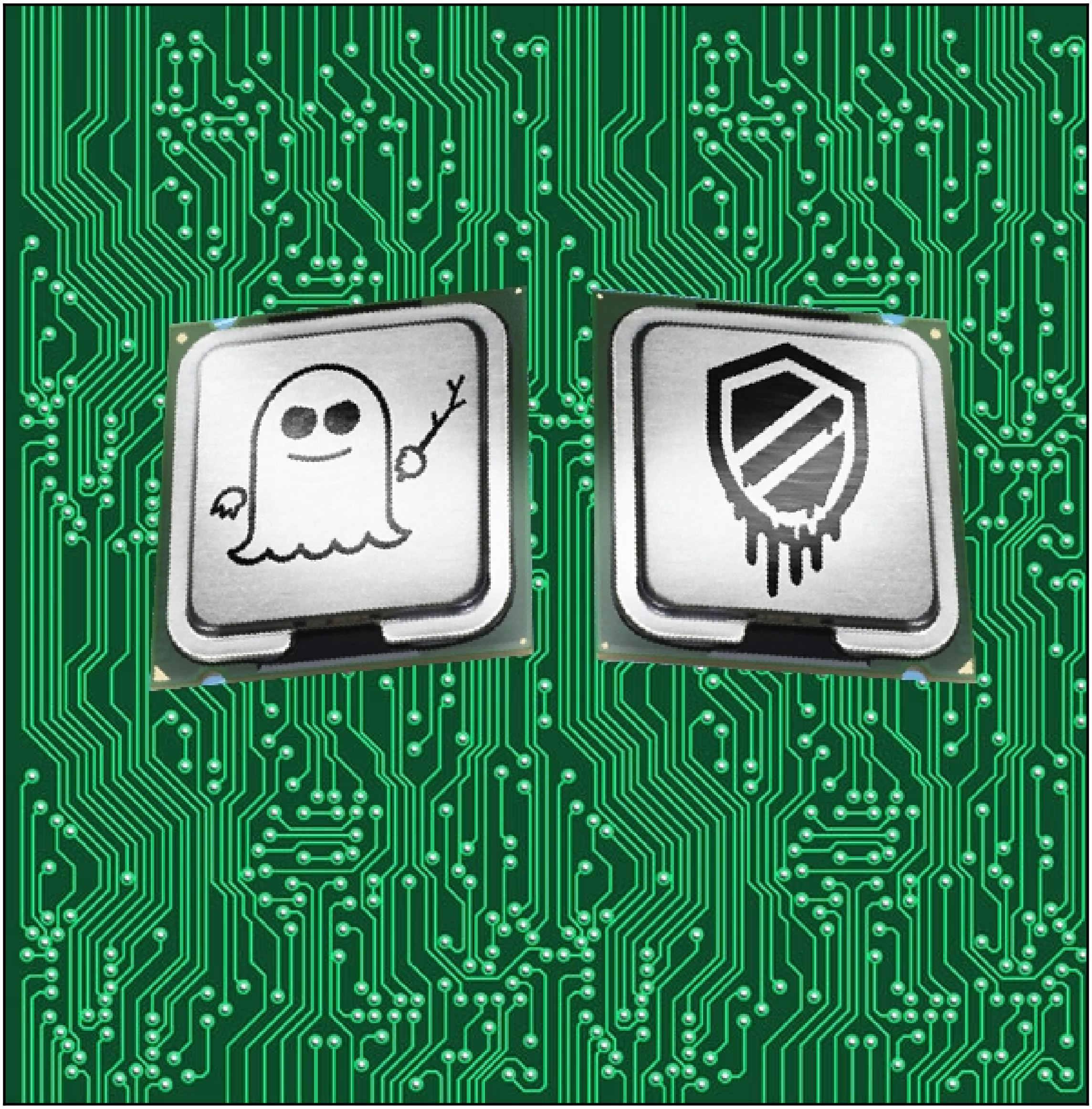
Managed by vendor

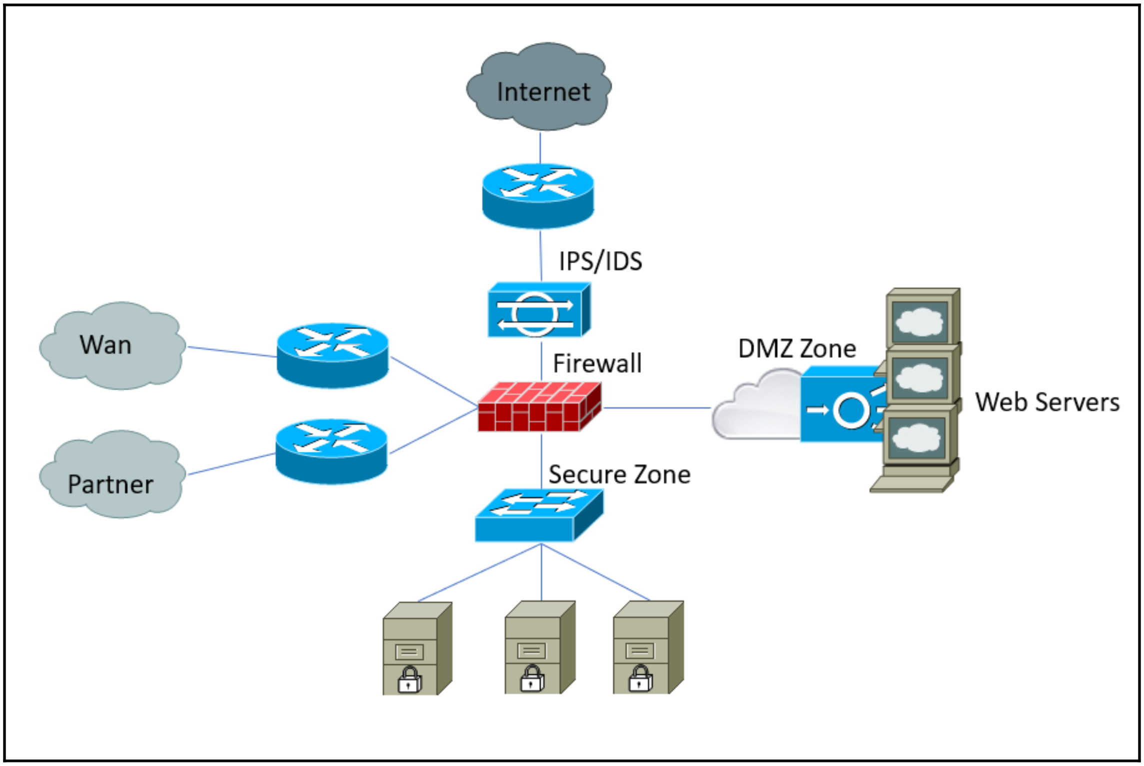
- Runtimes
- Security & Integration
- Databases
- Servers
- Virtualization
- Server HW
- Storage
- Networking

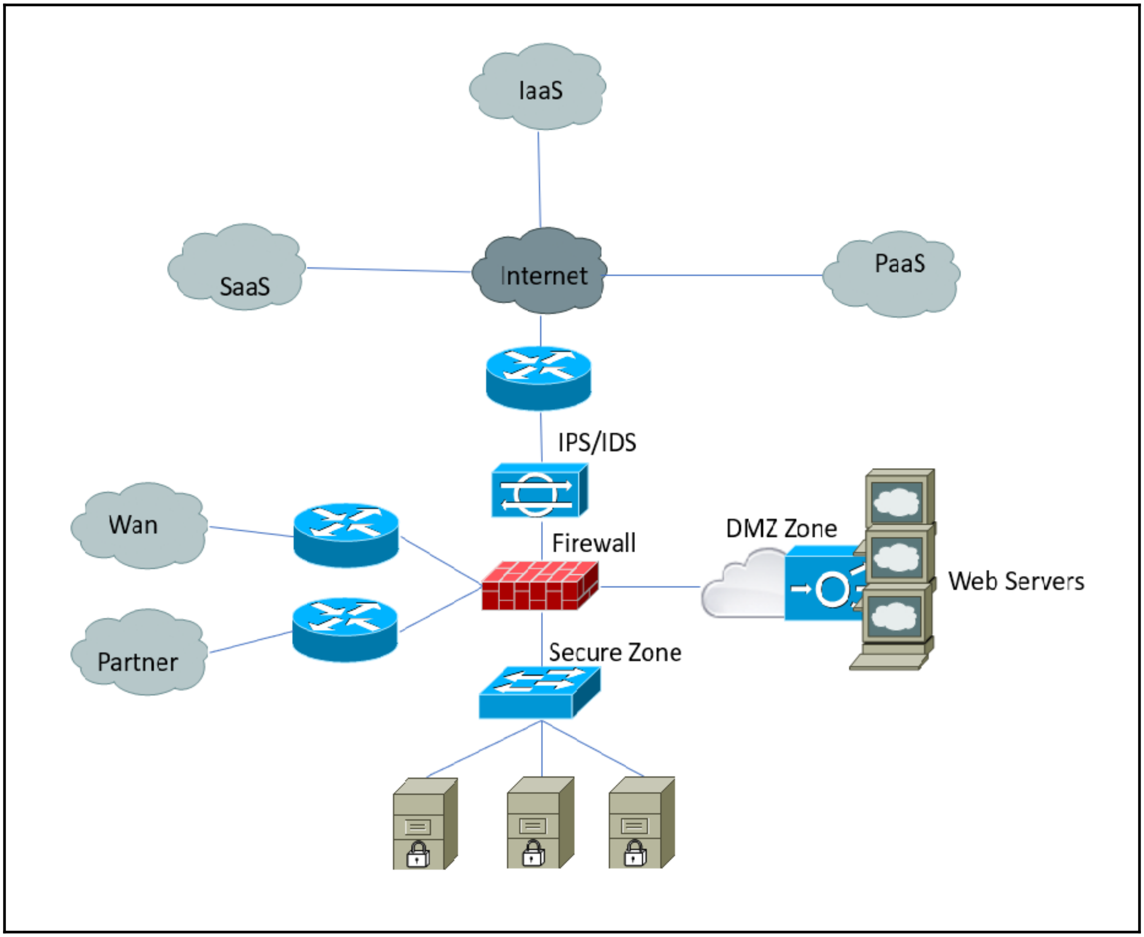
Software
(as a Service)

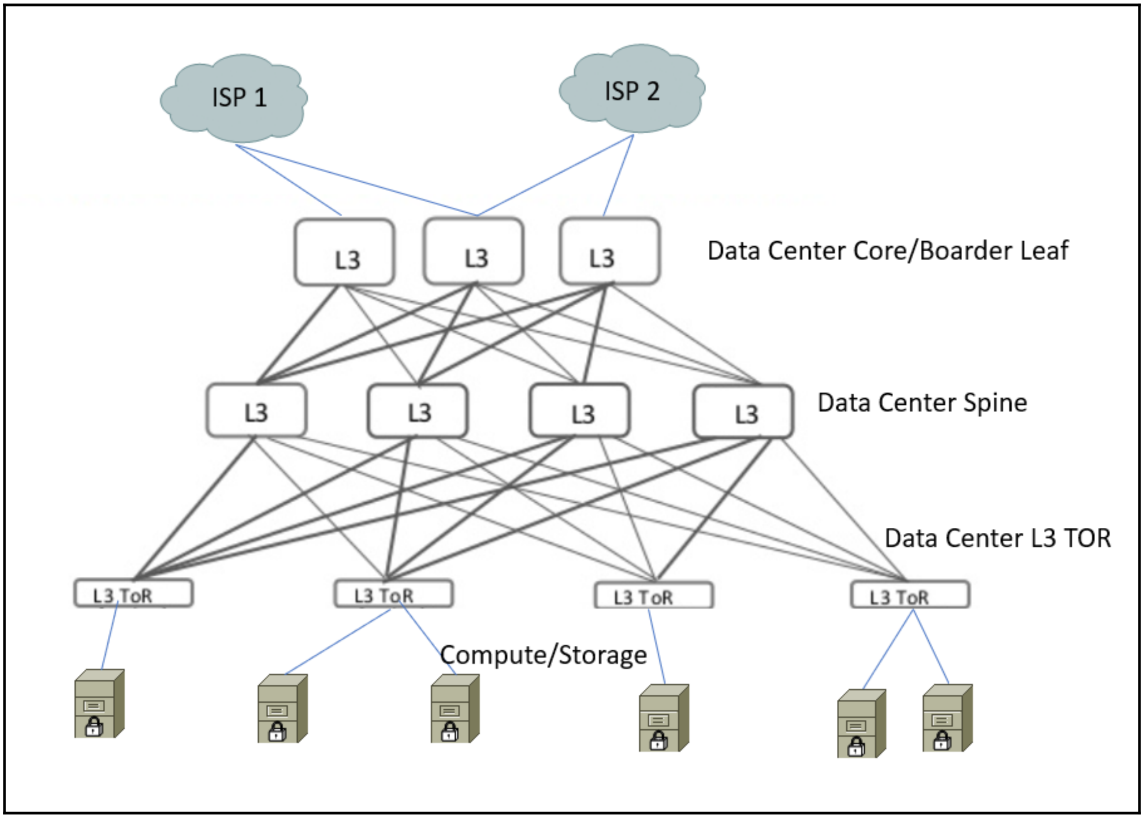
- Applications
- Runtimes
- Security & Integration
- Databases
- Servers
- Virtualization
- Server HW
- Storage
- Networking

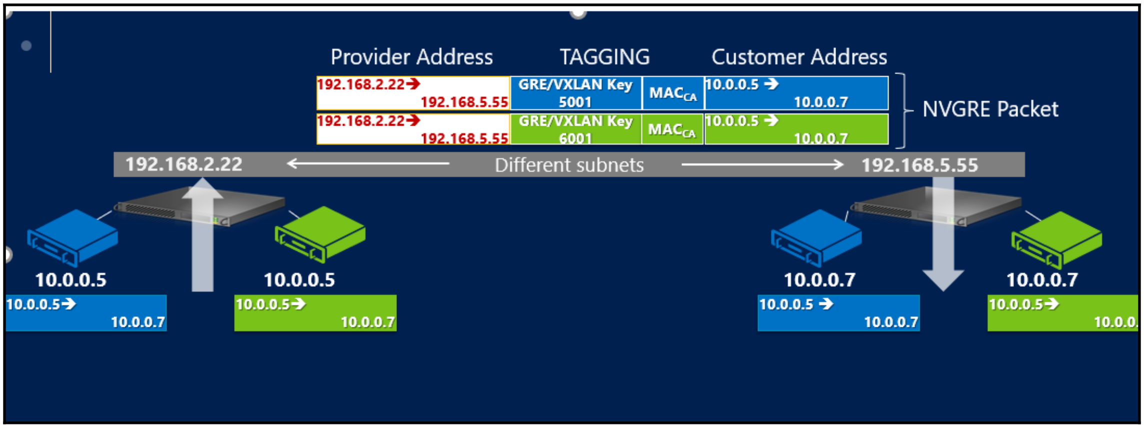

Compute
Networking
IaaS
Load-Balancing
Storage

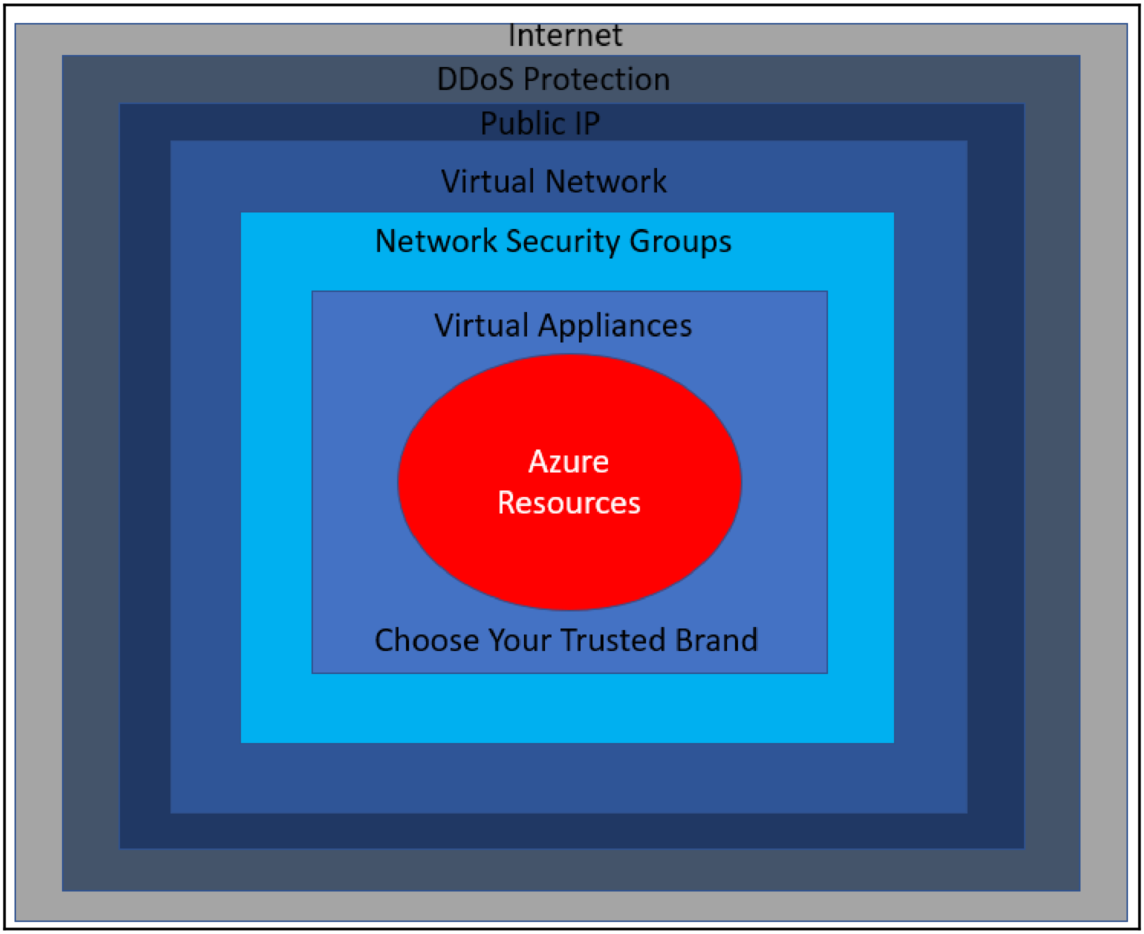


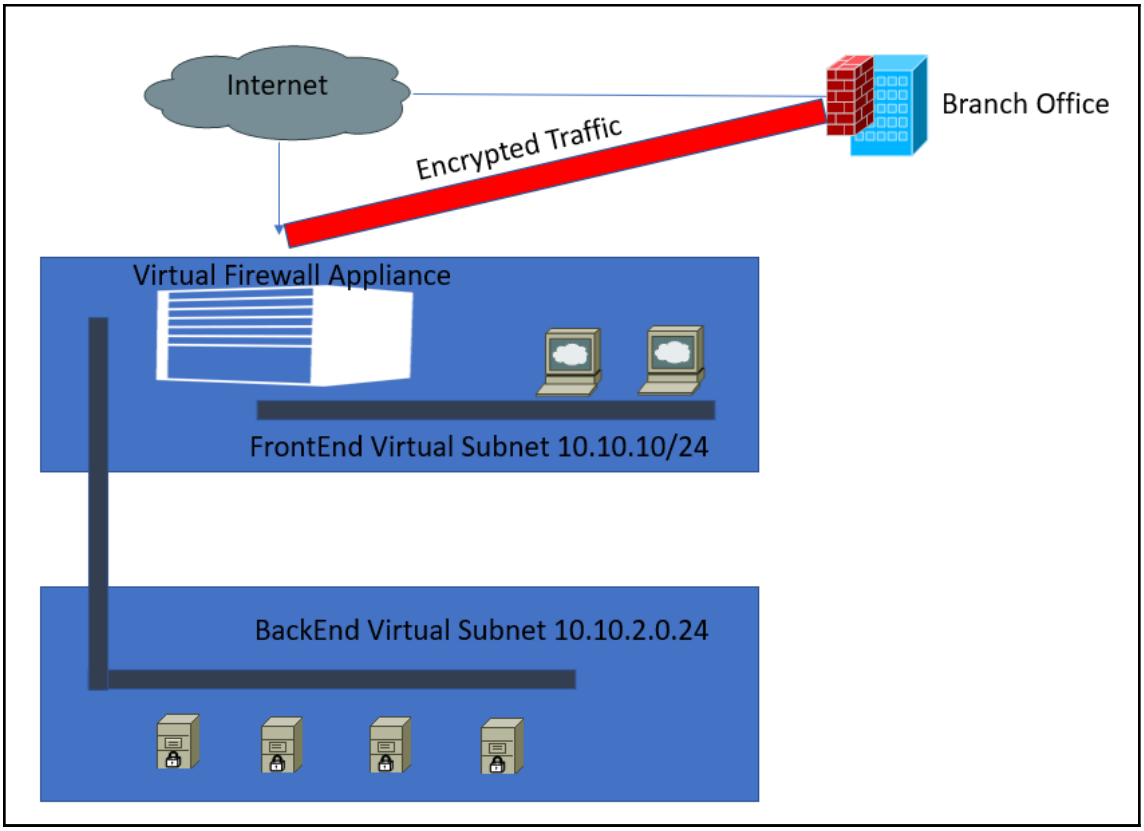

Internet
IPS/IDS
Wan
Firewall
DMZ Zone
Web Servers
Partner
Secure Zone

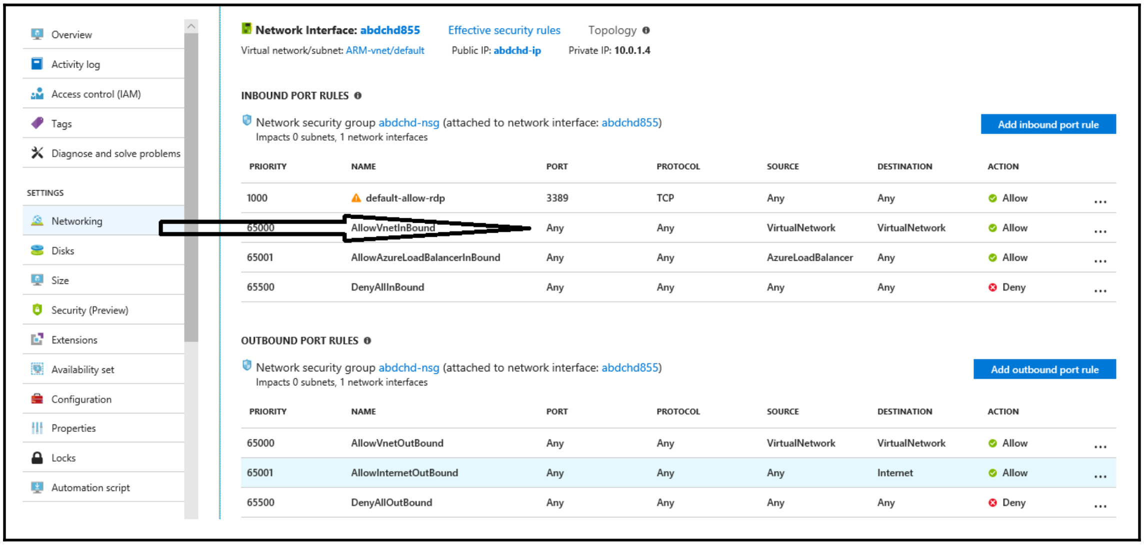

IaaS
SaaS
Internet
PaaS
IPS/IDS
Wan
Firewall
DMZ Zone
Web Servers
Partner
Secure Zone


ISP 1
ISP 2
L3
L3
L3
Data Center Core/Boarder Leaf
L3
L3
L3
L3
Data Center Spine
Data Center L3 TOR
L3 ToR
L3 ToR
L3 ToR
L3 ToR
Compute/Storage


Provider Address
TAGGING
Customer Address
192.168.2.22→ 192.168.5.55
GRE/VXLAN Key 5001
MACCA
10.0.0.5 → 10.0.0.7
192.168.2.22→ 192.168.5.55
GRE/VXLAN Key 6001
MACCA
10.0.0.5 → 10.0.0.7
NVGRE Packet
192.168.2.22
Different subnets
192.168.5.55
10.0.0.5
10.0.0.5→ 10.0.0.7
10.0.0.5
10.0.0.5→ 10.0.0.7
10.0.0.7
10.0.0.5 → 10.0.0.7
10.0.0.7
10.0.0.5→ 10.0.0.


Internet
DDoS Protection
Public IP
Virtual Network
Network Security Groups
Virtual Appliances
Azure Resources
Choose Your Trusted Brand


Internet
Branch Office
Encrypted Traffic
Virtual Firewall Appliance
FrontEnd Virtual Subnet 10.10.10/24
BackEnd Virtual Subnet 10.10.2.0.24



Network Interface: abdchd855

Virtual network/subnet: ARM-vnet/default Public IP: abdchd-ip Private IP: 10.0.1.4

INBOUND PORT RULES

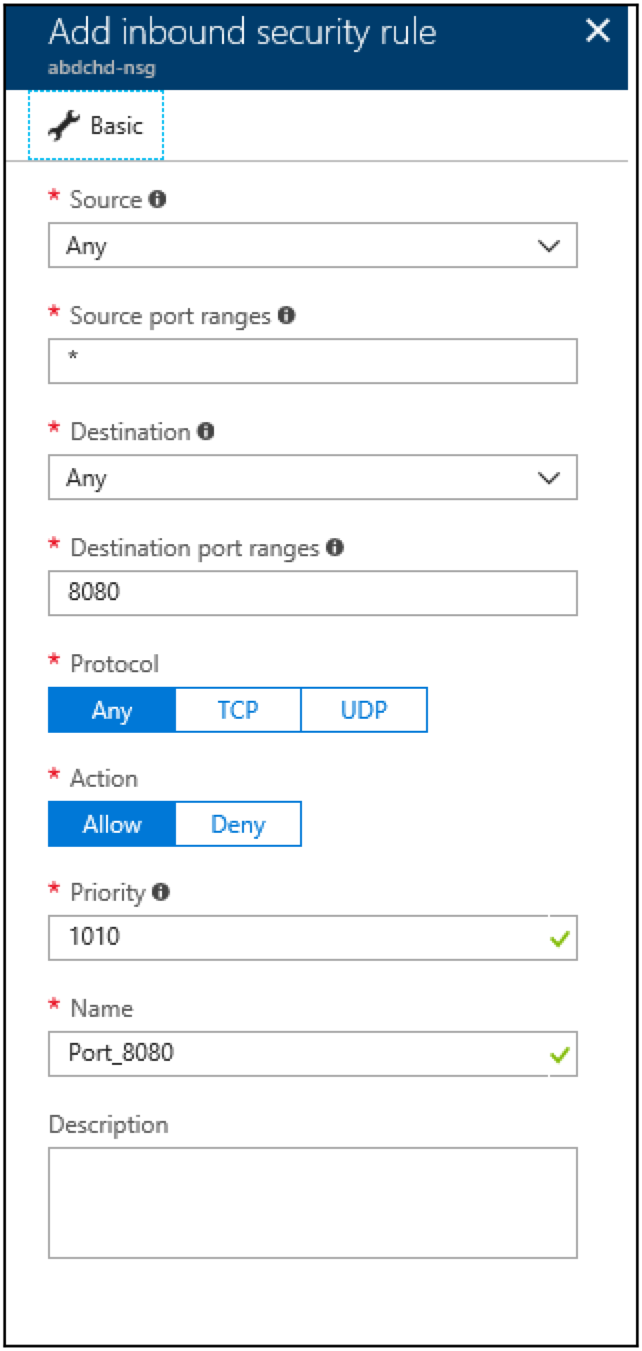
Network security group abdchd-nsg (attached to network interface: abdchd855)
Impacts 0 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
1000	⚠ default-allow-rdp	3389	TCP	Any	Any	✓ Allow	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow	...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny	...

OUTBOUND PORT RULES

Network security group abdchd-nsg (attached to network interface: abdchd855)
Impacts 0 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow	...
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow	...
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny	...



Add inbound security rule

abdchd-nsg

Basic

* Source: Any

* Source port ranges: *

* Destination: Any

* Destination port ranges: 8080

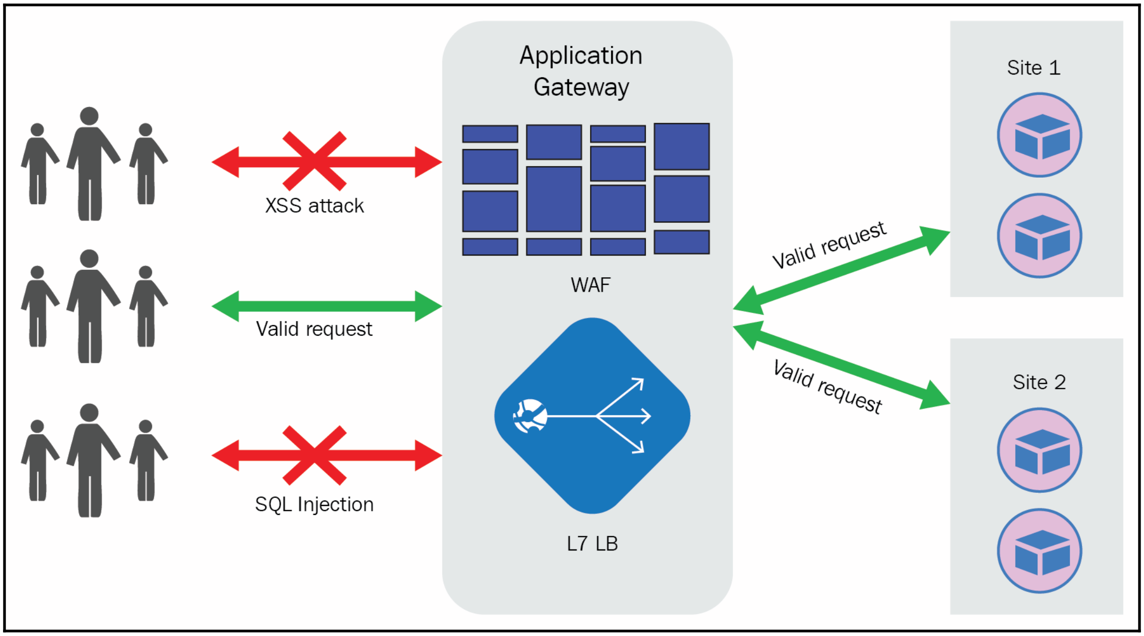
* Protocol: [✓ Any] TCP UDP

* Action: [✓ Allow] Deny

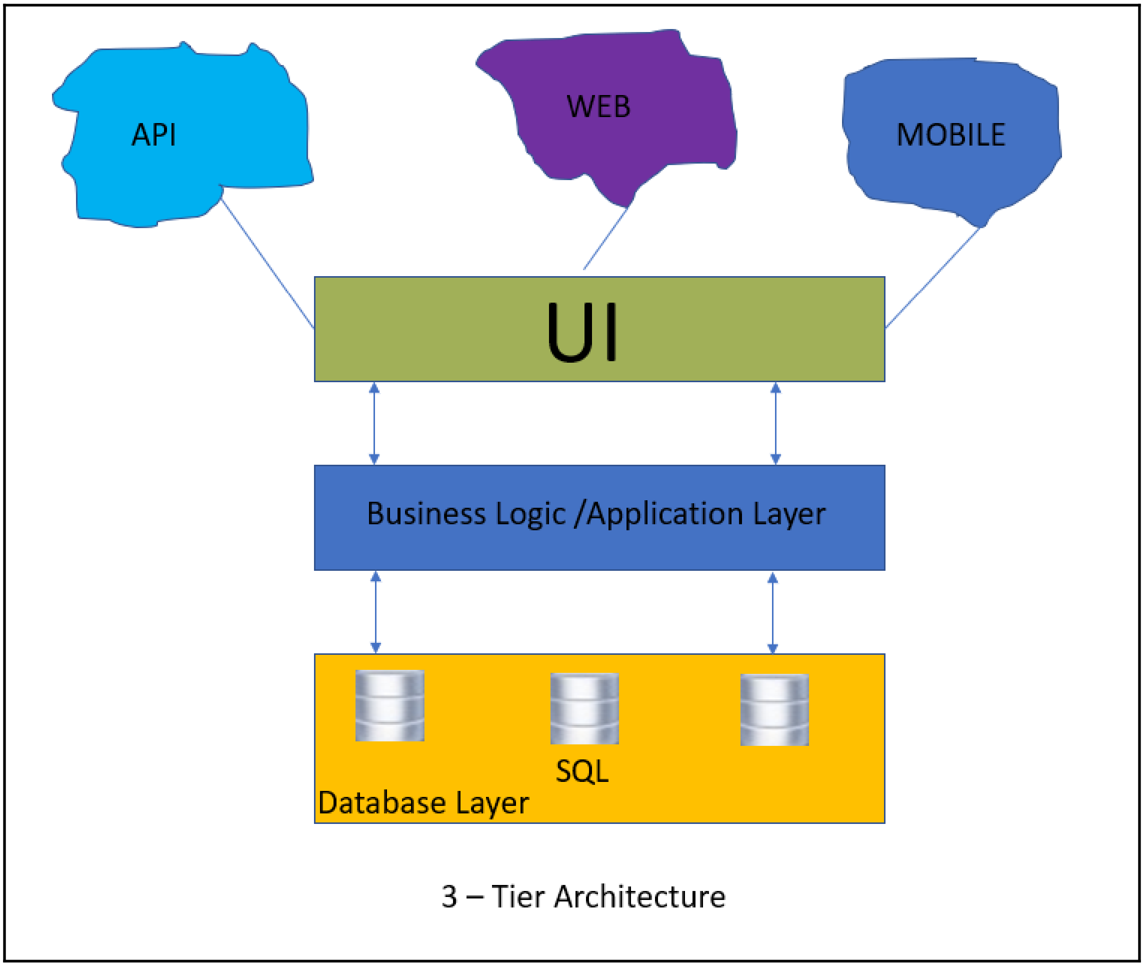
* Priority: 1010 ✓

* Name: Port_8080 ✓

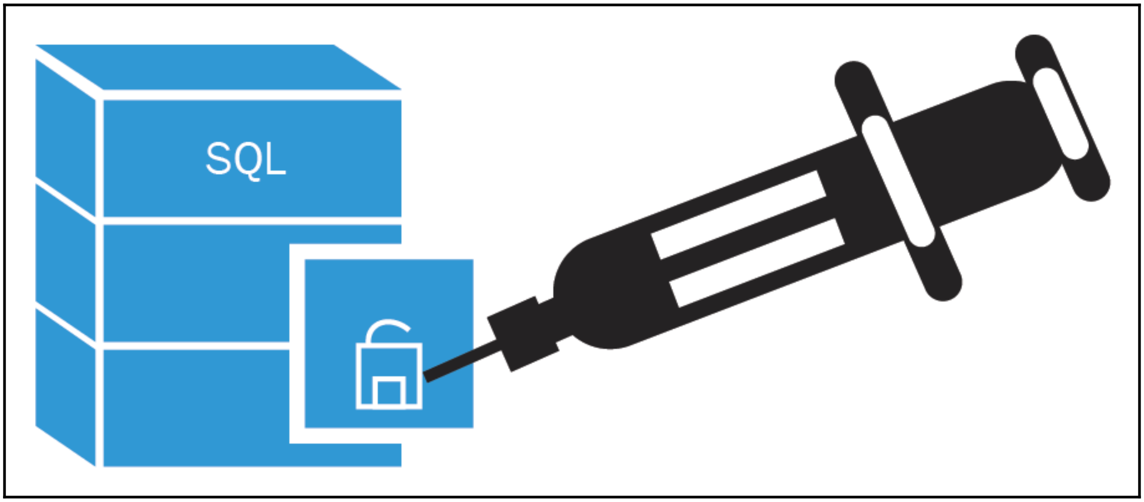
Description:

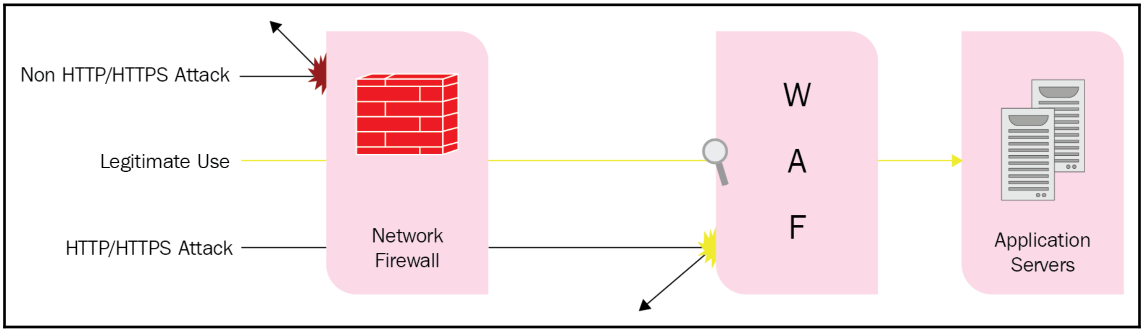

Application Gateway
XSS attack
Valid request
SQL Injection
WAF
L7 LB
Valid request
Valid request
Site 1
Site 2

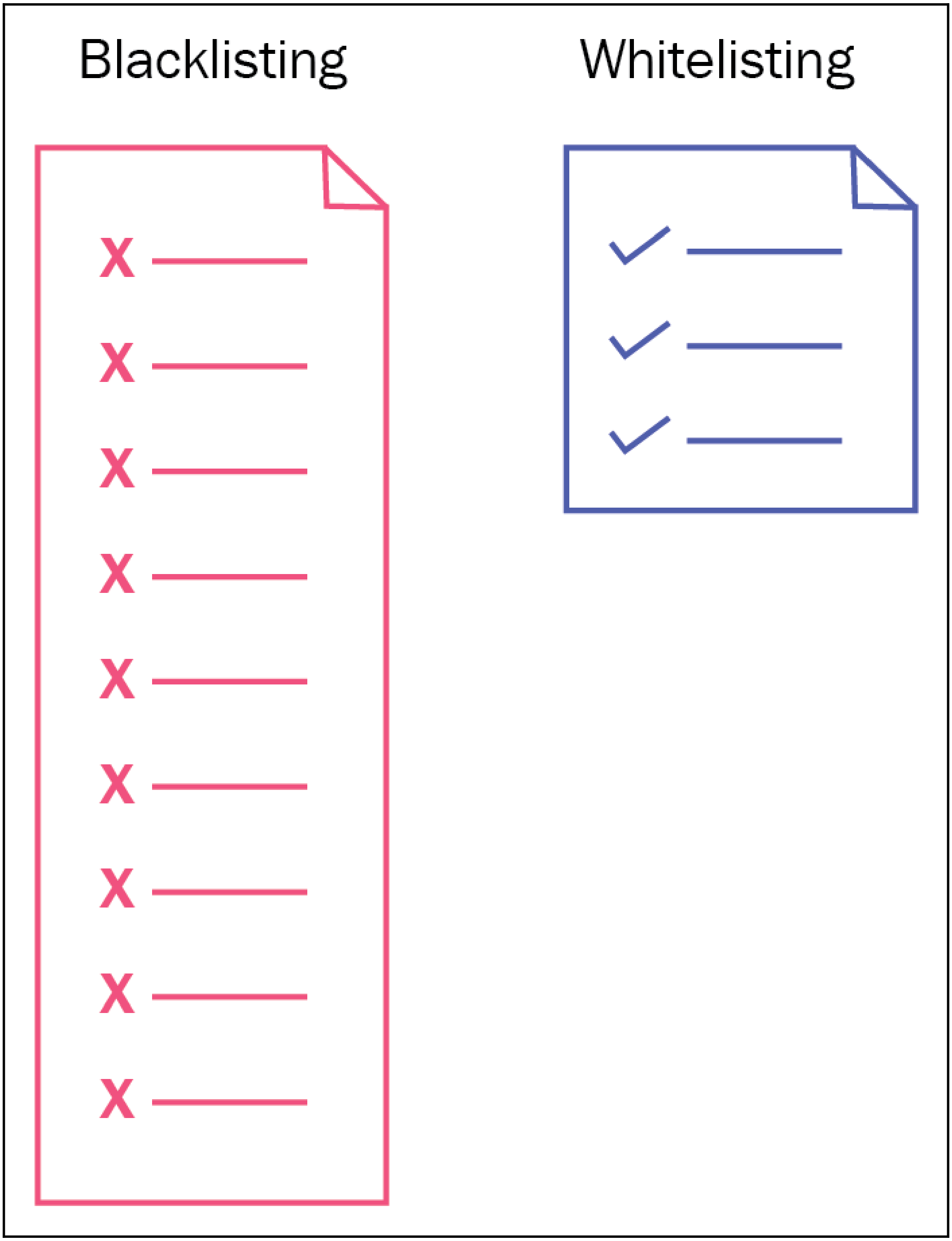
Chapter 5: Application Security Design

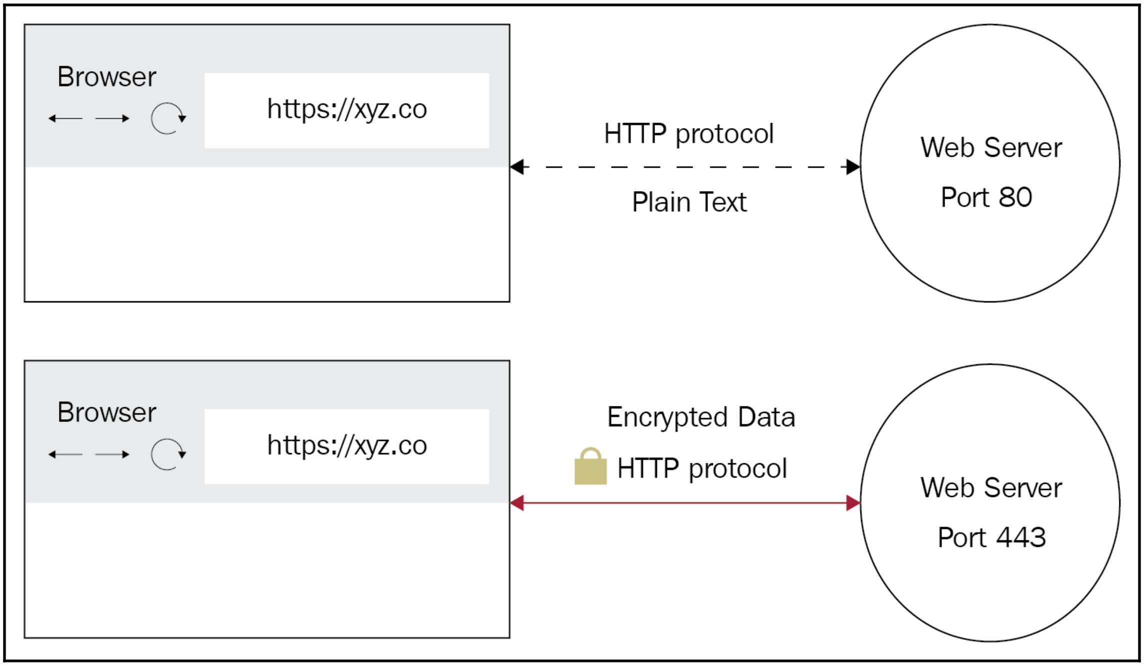


3 – Tier Architecture

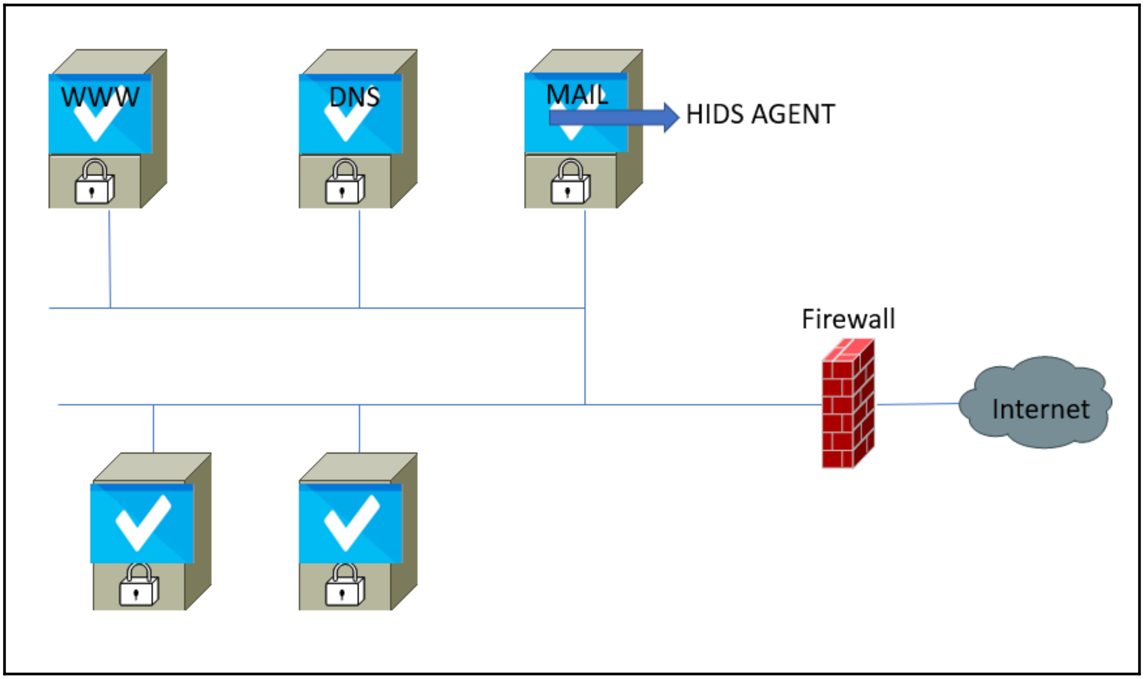

SQL

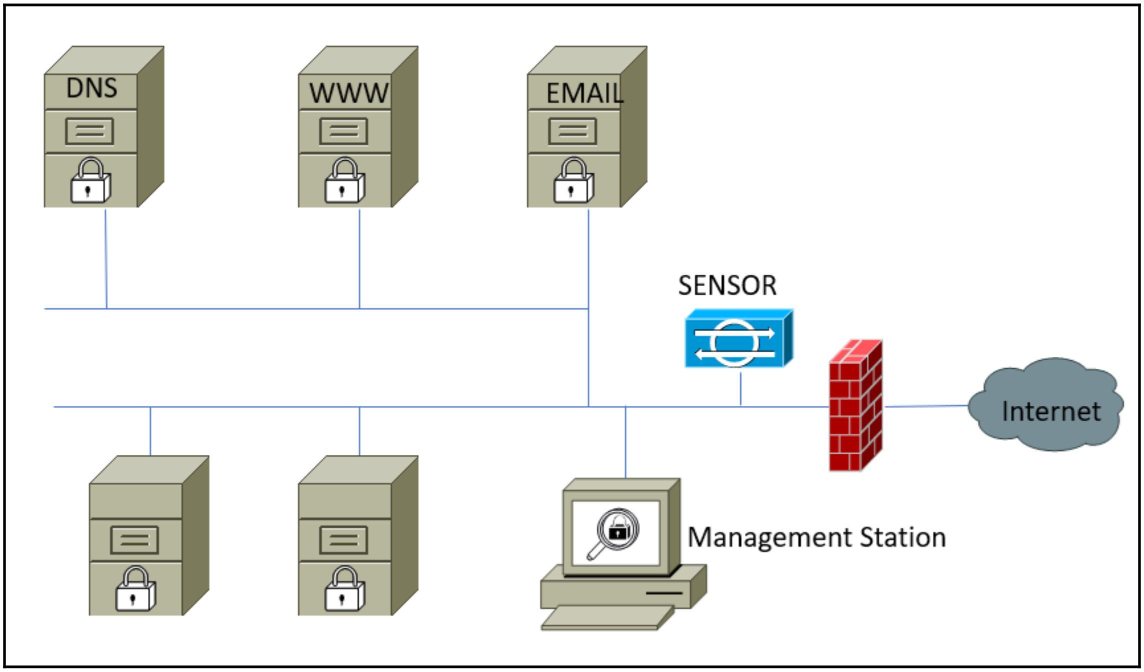

Non HTTP/HTTPS Attack
Legitimate Use
HTTP/HTTPS Attack
Network Firewall
W
A
F
Application Servers

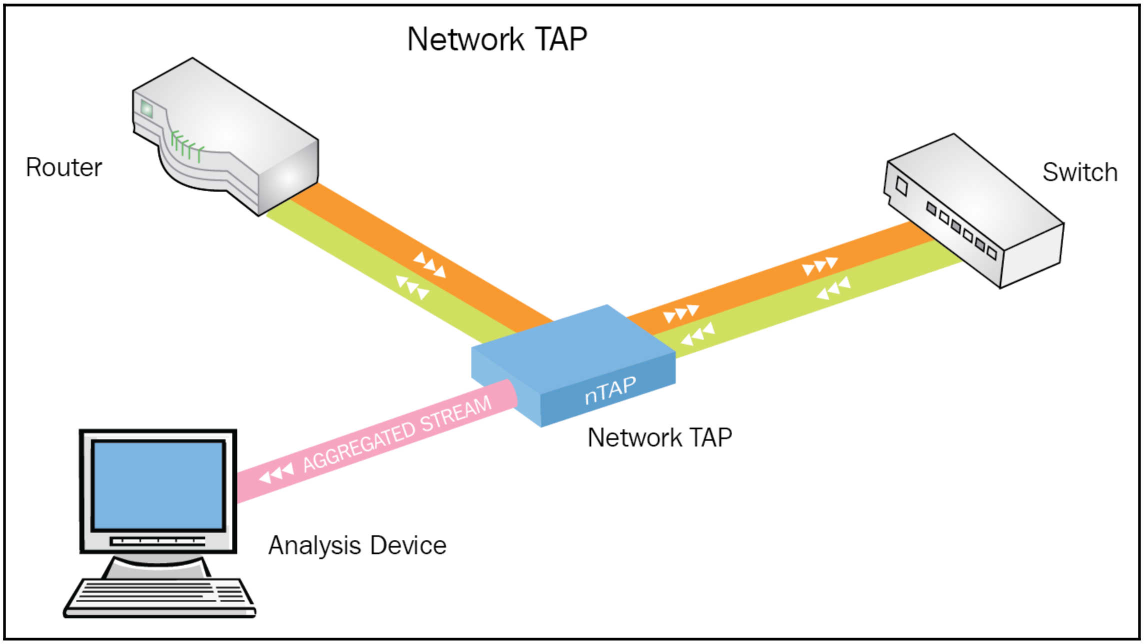

Blacklisting
Whitelisting

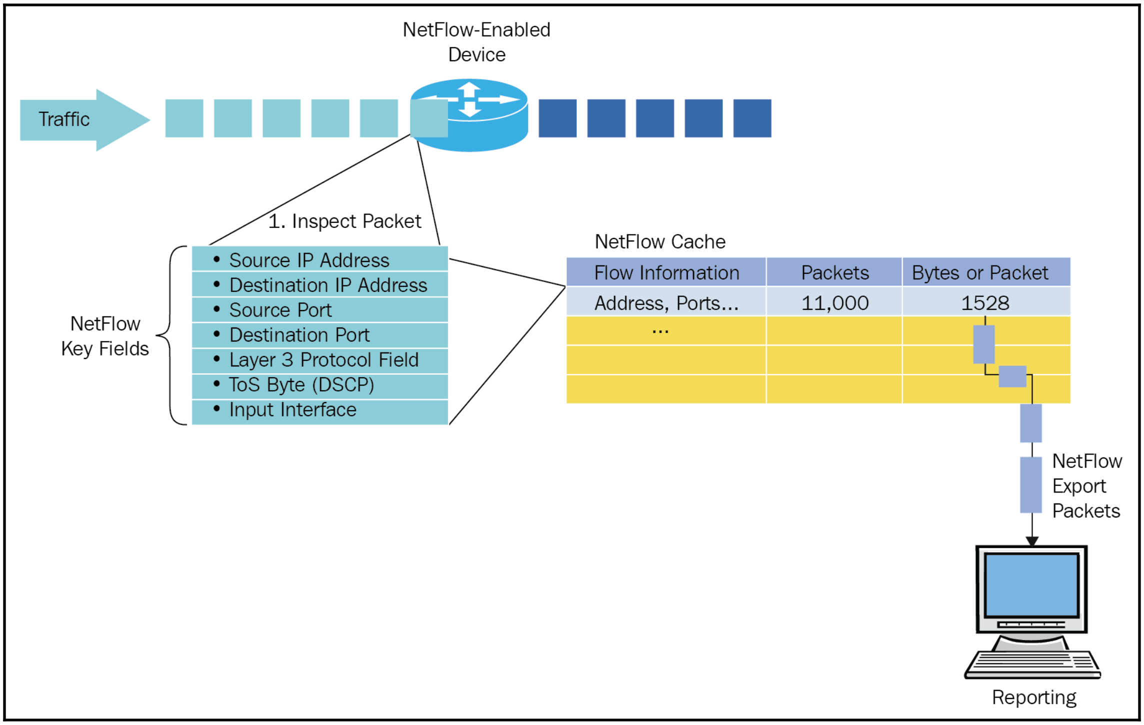

Browser
https://xyz.co
HTTP protocol
Plain Text
Web Server
Port 80
Browser
https://xyz.co
Encrypted Data
HTTP protocol
Web Server
Port 443

Chapter 6: Threat Detection and Response

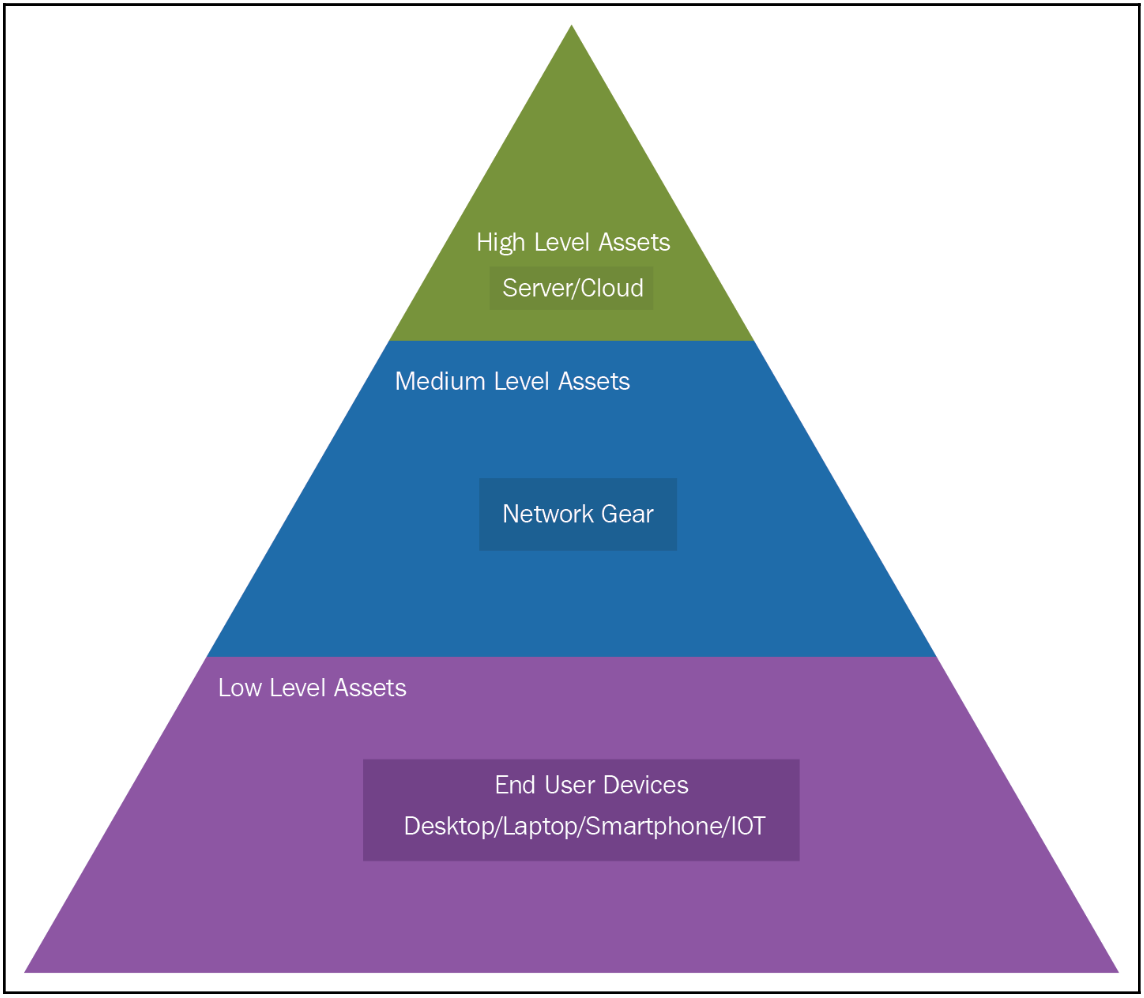


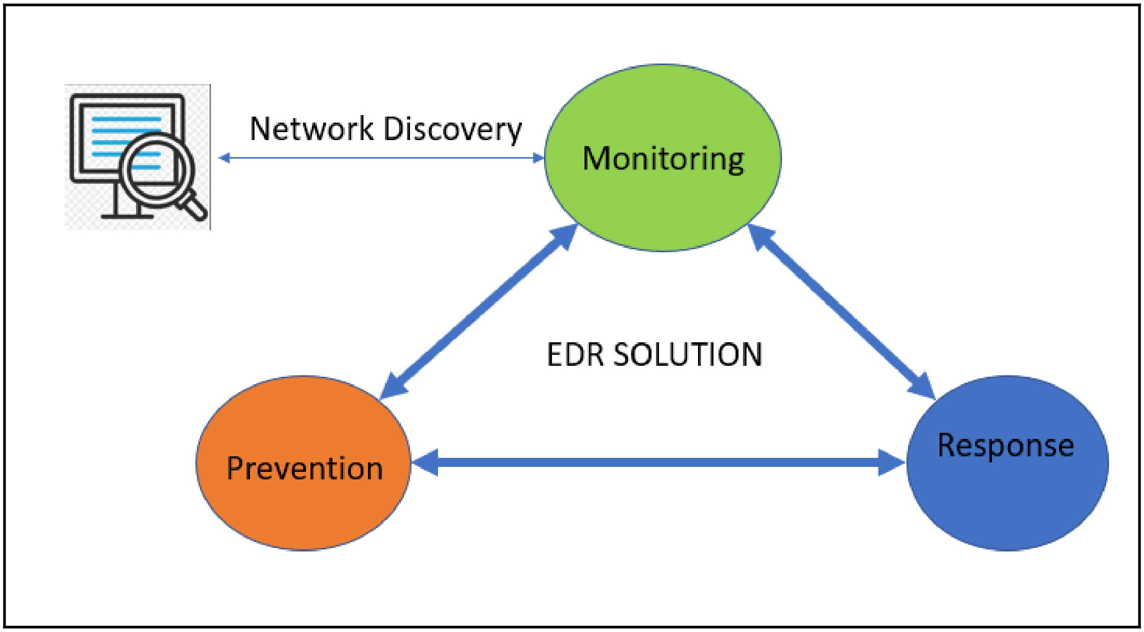

DNS
WWW
EMAIL
SENSOR
Internet
Management Station

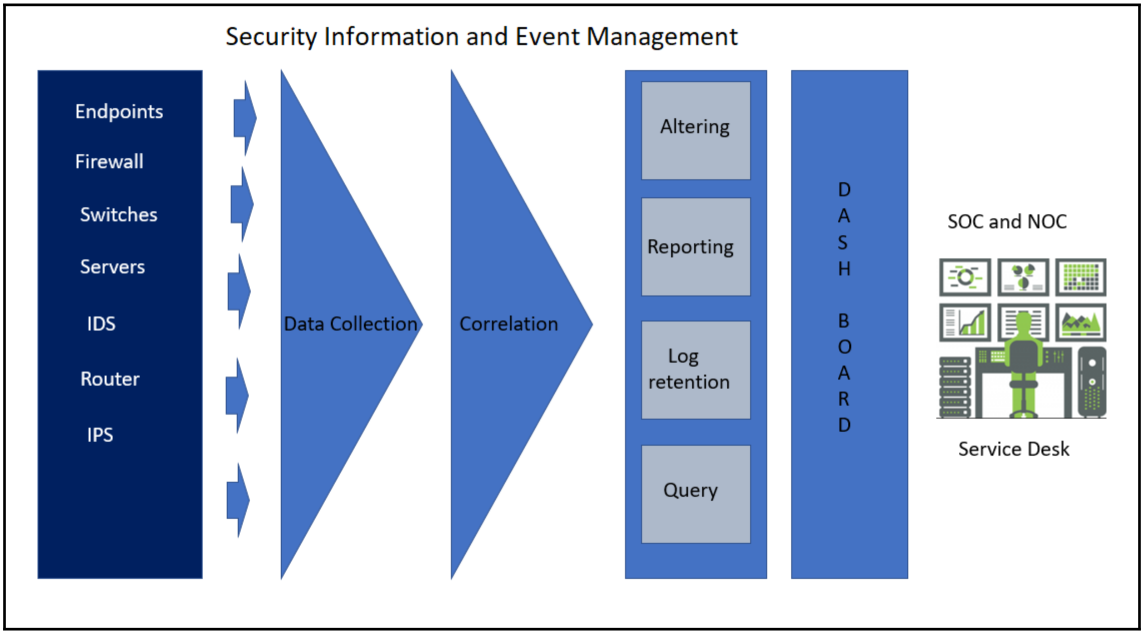

Network TAP
Router
Switch
nTAP
AGGREGATED STREAM
Network TAP
Analysis Device

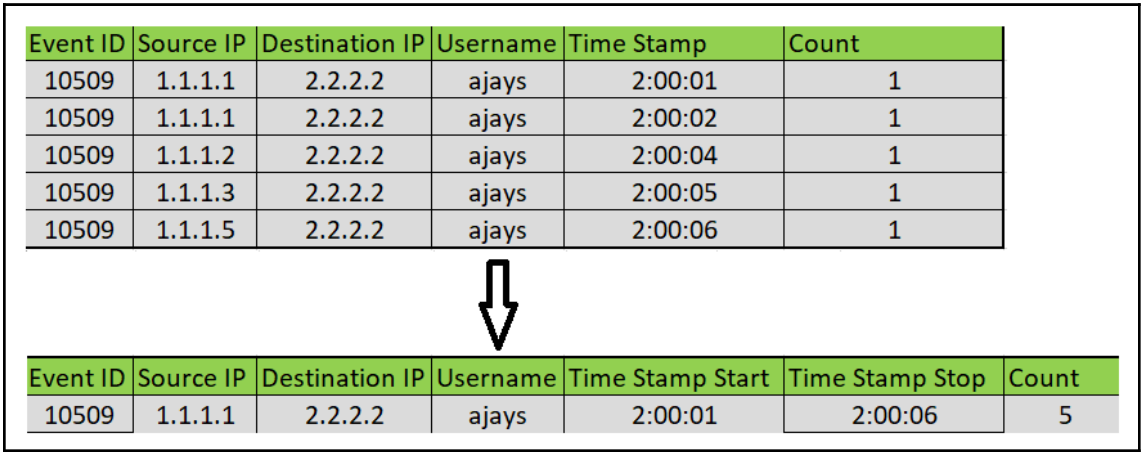


Flow Information	Packets	Bytes or Packet
Address, Ports...	11,000	1528
...		


High Level Assets
Server/Cloud
Medium Level Assets
Network Gear
Low Level Assets
End User Devices
Desktop/Laptop/Smartphone/IOT

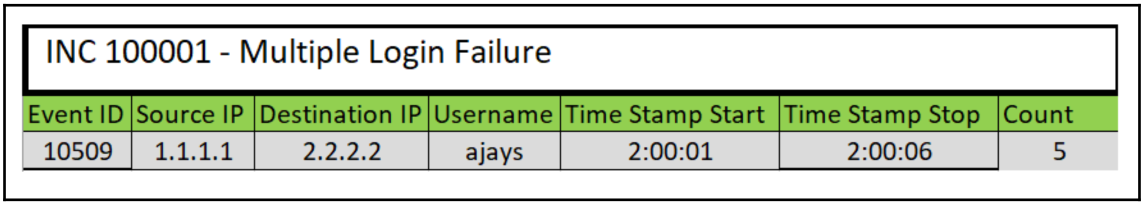

Network Discovery
Monitoring
EDR SOLUTION
Prevention
Response


Security Information and Event Management
Endpoints
Firewall
Switches
Servers
IDS
Router
IPS
Data Collection
Correlation
Altering
Reporting
Log retention
Query
DASHBOARD
SOC and NOC
Service Desk



Event ID	Source IP	Destination IP	Username	Time Stamp	Count
10509	1.1.1.1	2.2.2.2	ajays	2:00:01	1
10509	1.1.1.1	2.2.2.2	ajays	2:00:02	1
10509	1.1.1.2	2.2.2.2	ajays	2:00:04	1
10509	1.1.1.3	2.2.2.2	ajays	2:00:05	1
10509	1.1.1.5	2.2.2.2	ajays	2:00:06	1

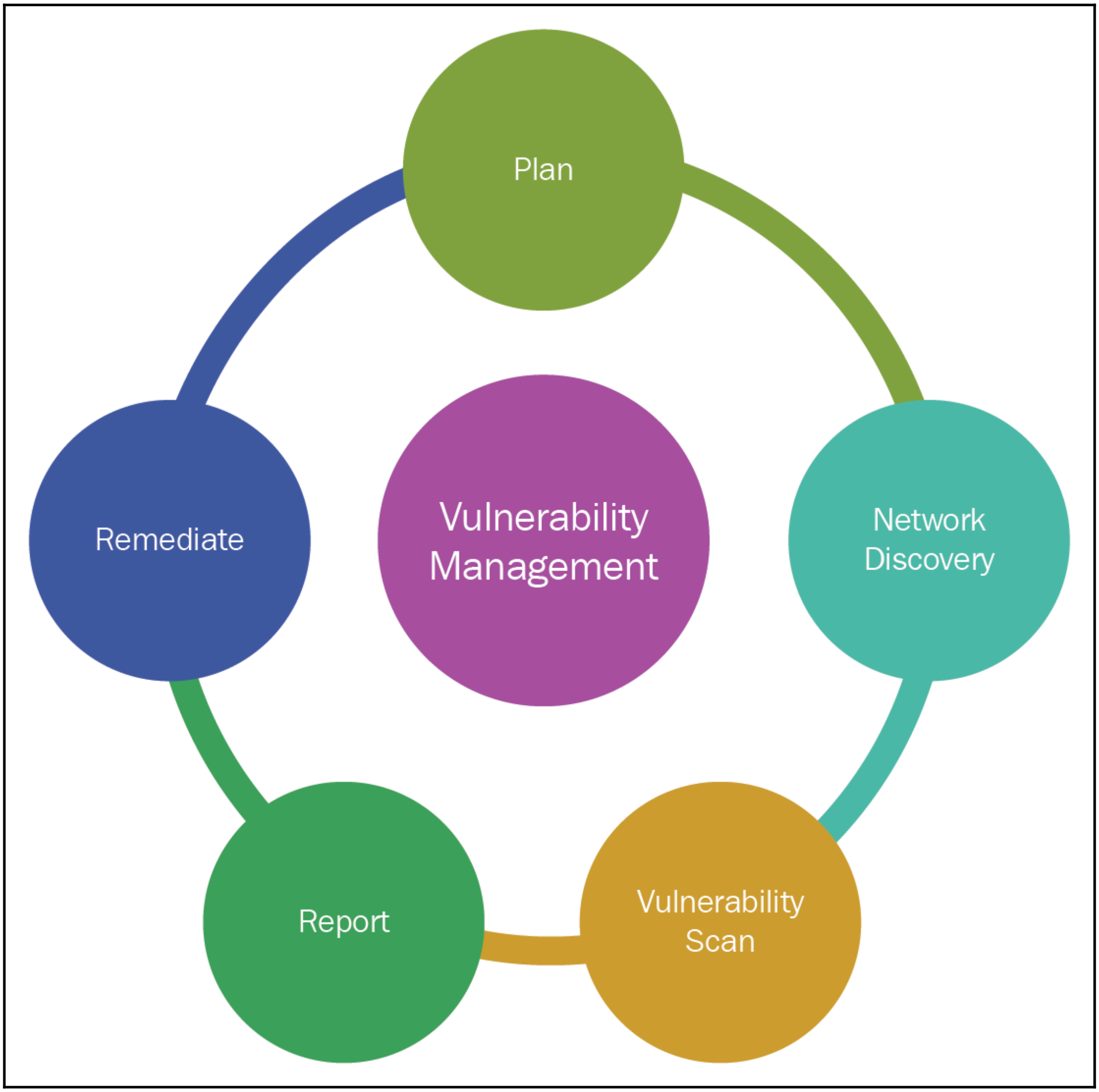
Event ID	Source IP	Destination IP	Username	Time Stamp Start	Time Stamp Stop	Count
10509	1.1.1.1	2.2.2.2	ajays	2:00:01	2:00:06	5

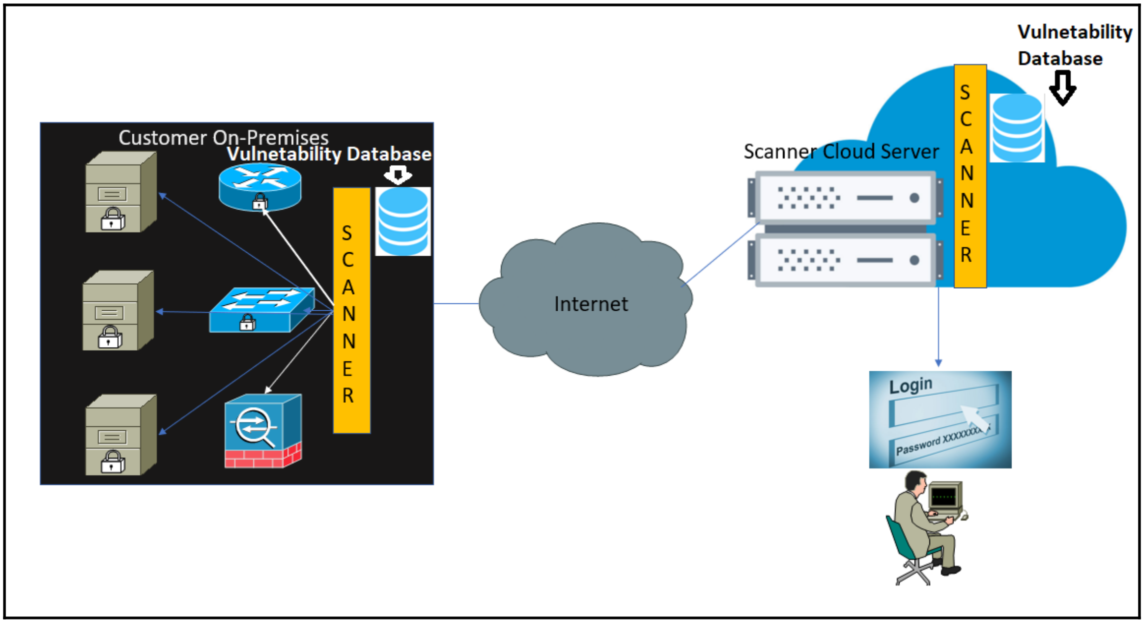


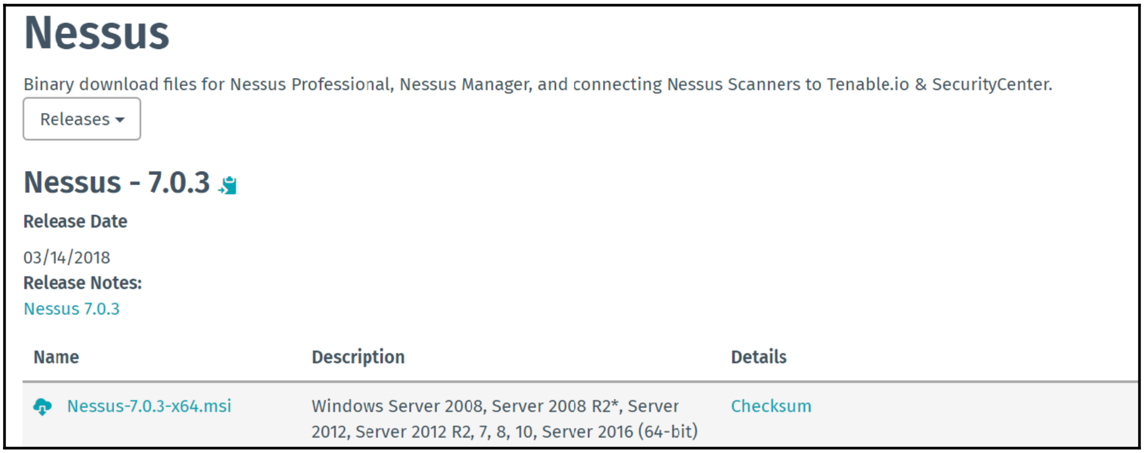
INC 100001 - Multiple Login Failure

Event ID	Source IP	Destination IP	Username	Time Stamp Start	Time Stamp Stop	Count
10509	1.1.1.1	2.2.2.2	ajays	2:00:01	2:00:06	5

Chapter 7: Vulnerability Assessment







Nessus

Binary download files for Nessus Professional, Nessus Manager, and connecting Nessus Scanners to Tenable.io & SecurityCenter.

Nessus - 7.0.3

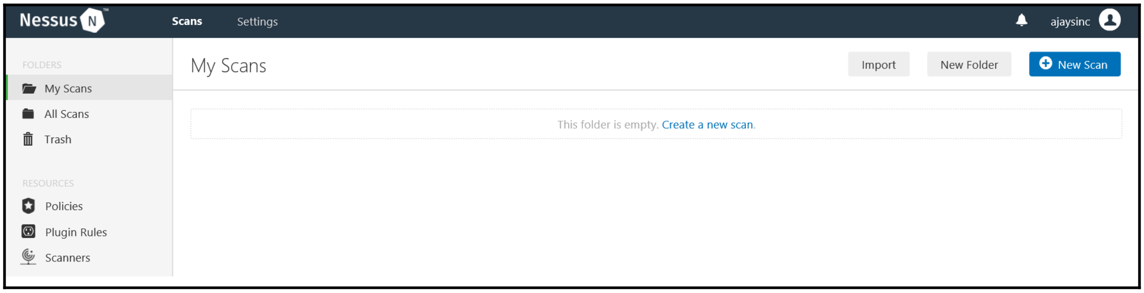
Release Date

03/14/2018

Release Notes:

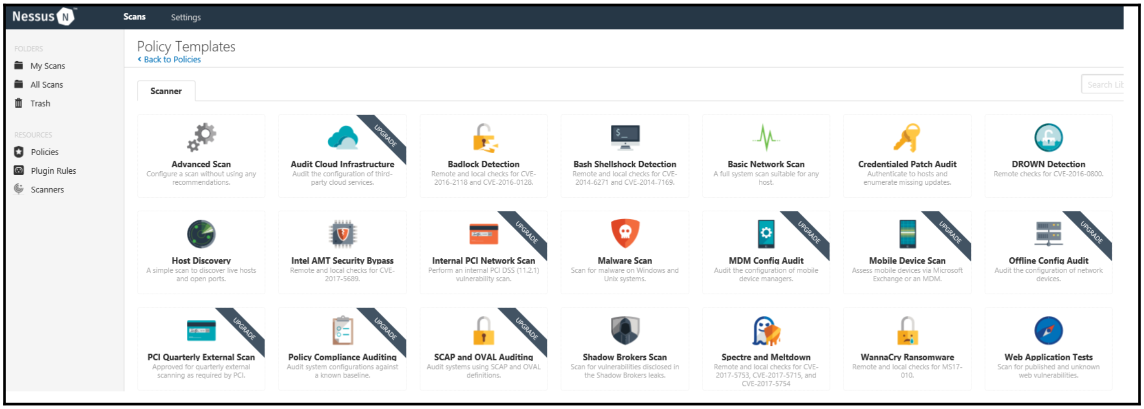
Nessus 7.0.3

Name	Description	Details
Nessus-7.0.3-x64.msi	Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016 (64-bit)	Checksum



My Scans

This folder is empty. Create a new scan.



Policy Templates

Advanced Scan Configure a scan without using any recommendations.

Audit Cloud Infrastructure Audit the configuration of third-party cloud services.

Badlock Detection Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Basic Network Scan A full system scan suitable for any host.

Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.

DROWN Detection Remote checks for CVE-2016-0800.

Host Discovery A simple scan to discover live hosts and open ports.

Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.

Internal PCI Network Scan Perform an internal PCI DSS (11.2.1) vulnerability scan.

Malware Scan Scan for malware on Windows and Unix systems.

MDM Config Audit Audit the configuration of mobile device managers.

Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM.

Offline Config Audit Audit the configuration of network devices.

PCI Quarterly External Scan Approved for quarterly external scanning as required by PCI.

Policy Compliance Auditing Audit system configurations against a known baseline.

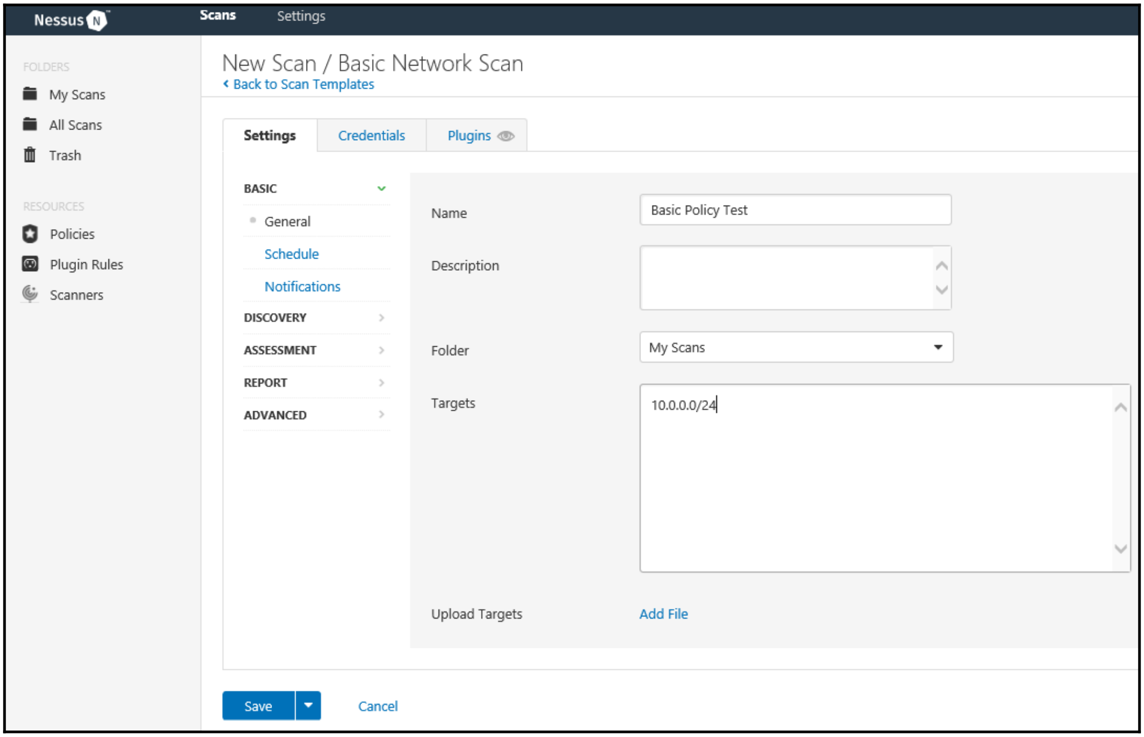
SCAP and OVAL Auditing Audit systems using SCAP and OVAL definitions.

Shadow Brokers Scan Scan for vulnerabilities disclosed in the Shadow Brokers leaks.

Spectre and Meltdown Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware Remote and local checks for MS17-010.

Web Application Tests Scan for published and unknown web vulnerabilities.



New Scan / Basic Network Scan

‹ Back to Scan Templates

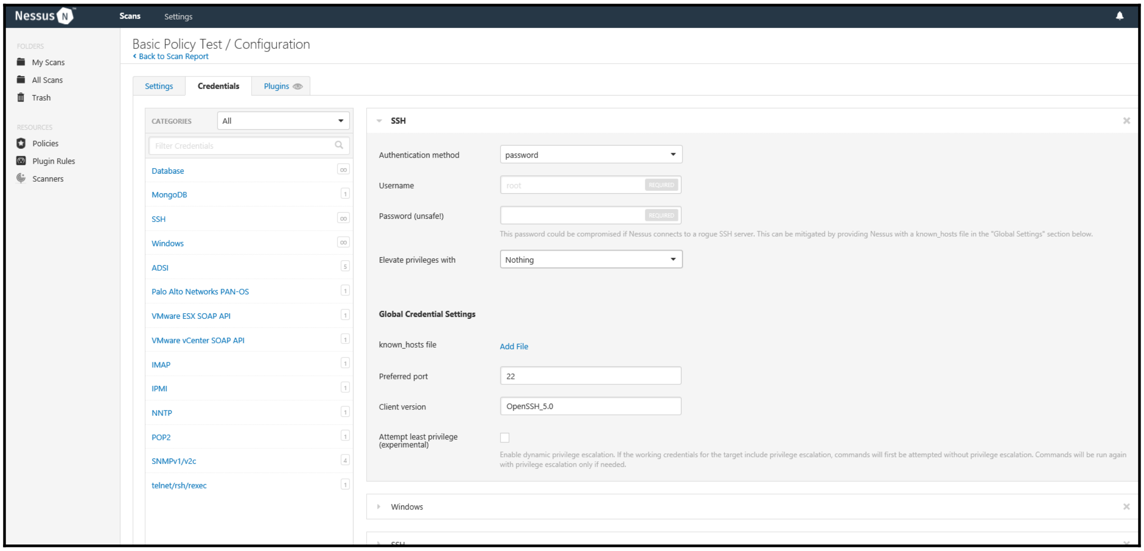
Name: Basic Policy Test

Description:

Folder: My Scans

Targets: 10.0.0.0/24

Upload Targets: Add File



Basic Policy Test / Configuration

‹ Back to Scan Report

Database	∞
MongoDB	1
SSH	∞
Windows	∞
ADSI	5
Palo Alto Networks PAN-OS	1
VMware ESX SOAP API	1
VMware vCenter SOAP API	1
IMAP	1
IPMI	1
NNTP	1
POP2	1
SNMPv1/v2c	4
telnet/rsh/rexec	1

SSH

Authentication method: password

Username: root REQUIRED

Password (unsafe!): REQUIRED

This password could be compromised if Nessus connects to a rogue SSH server. This can be mitigated by providing Nessus with a known_hosts file in the "Global Settings" section below.

Elevate privileges with: Nothing

Global Credential Settings

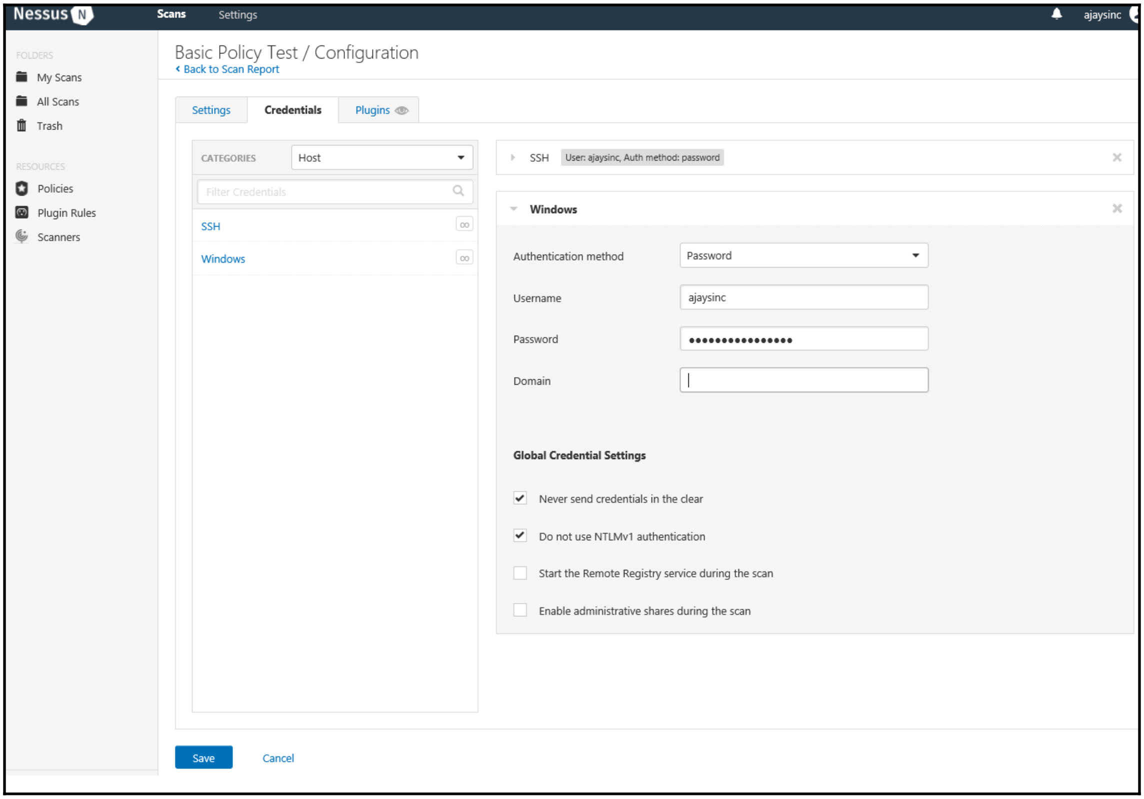
known_hosts file: Add File

Preferred port: 22

Client version: OpenSSH_5.0

Attempt least privilege (experimental): □

Enable dynamic privilege escalation. If the working credentials for the target include privilege escalation, commands will first be attempted without privilege escalation. Commands will be run again with privilege escalation only if needed.



Basic Policy Test / Configuration

CATEGORIES: Host

SSH User: ajaysinc, Auth method: password

Windows

Authentication method	Password
Username	ajaysinc
Password	●●●●●●●●●●●●●●●●
Domain	

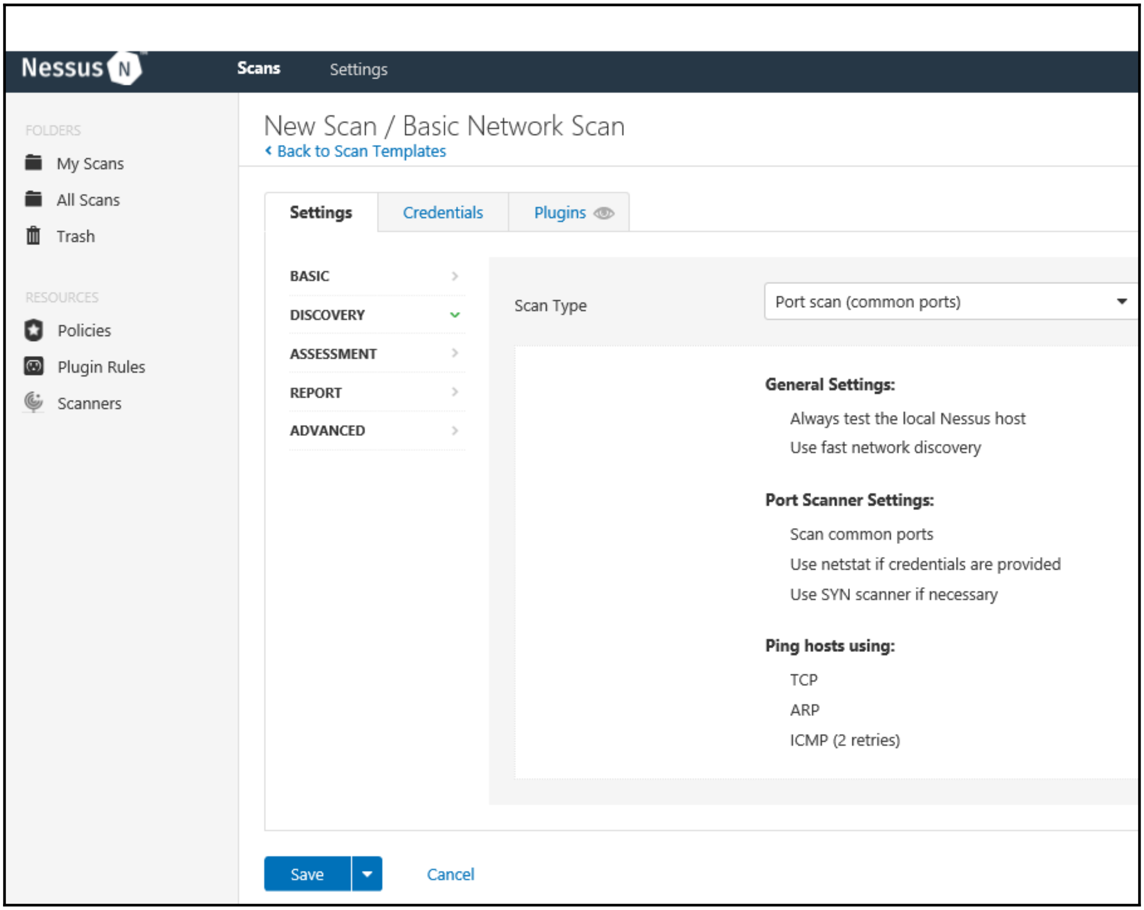
Global Credential Settings

☑ Never send credentials in the clear

☑ Do not use NTLMv1 authentication

□ Start the Remote Registry service during the scan

□ Enable administrative shares during the scan



New Scan / Basic Network Scan

‹ Back to Scan Templates

Scan Type: Port scan (common ports)

General Settings:

Always test the local Nessus host

Use fast network discovery

Port Scanner Settings:

Scan common ports

Use netstat if credentials are provided

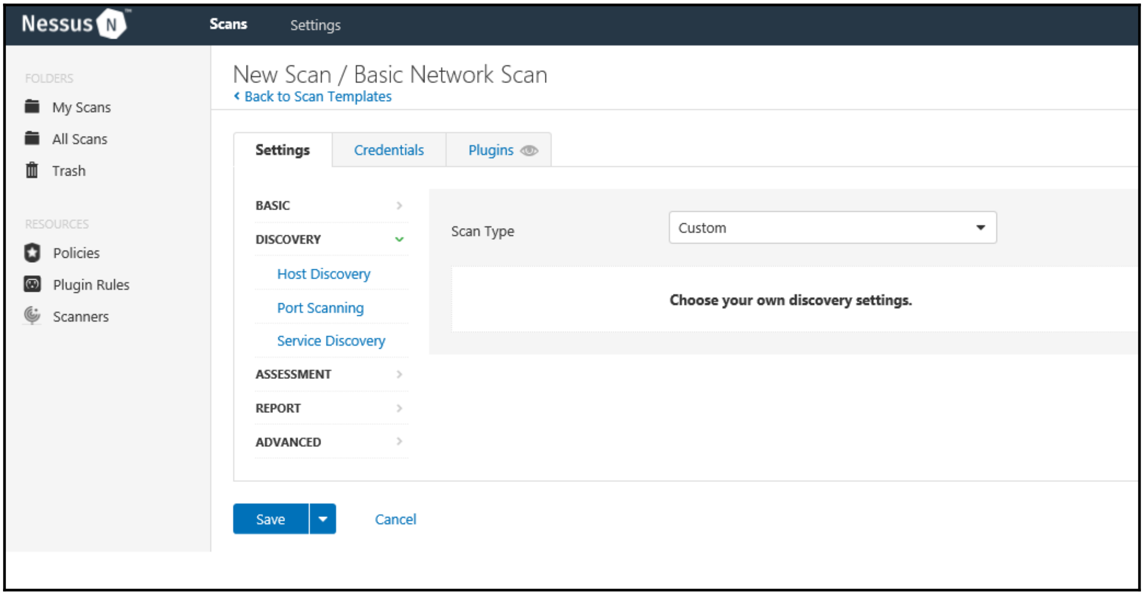
Use SYN scanner if necessary

Ping hosts using:

TCP

ARP

ICMP (2 retries)

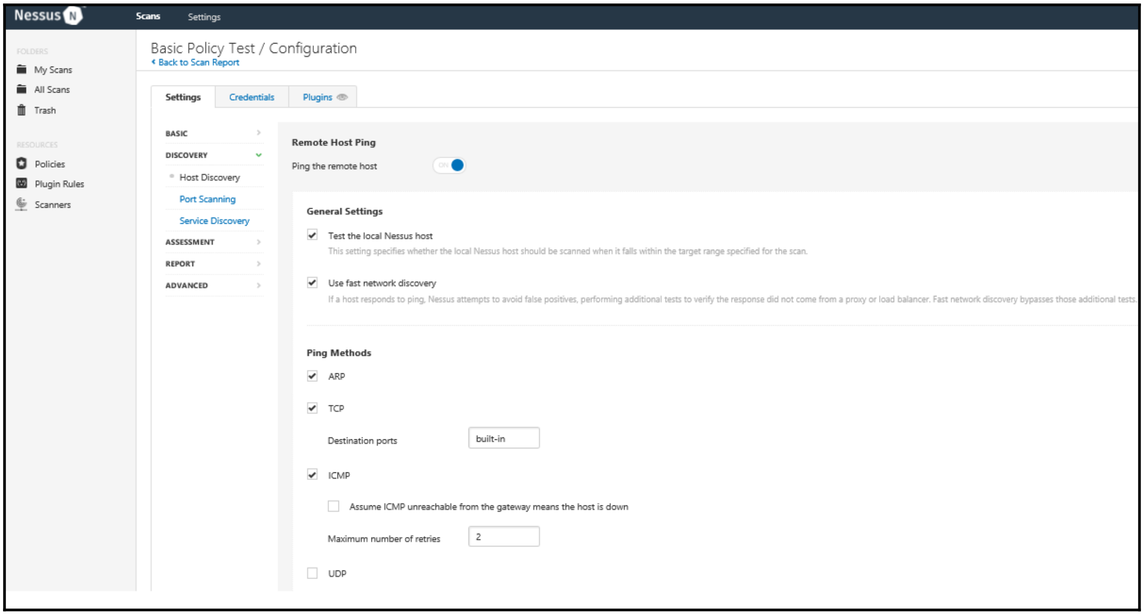


New Scan / Basic Network Scan

‹ Back to Scan Templates

Scan Type: Custom

Choose your own discovery settings.



Basic Policy Test / Configuration

‹ Back to Scan Report

Remote Host Ping

Ping the remote host: ON

General Settings

☑ Test the local Nessus host

This setting specifies whether the local Nessus host should be scanned when it falls within the target range specified for the scan.

☑ Use fast network discovery

If a host responds to ping, Nessus attempts to avoid false positives, performing additional tests to verify the response did not come from a proxy or load balancer. Fast network discovery bypasses those additional tests.

Ping Methods

☑ ARP

☑ TCP

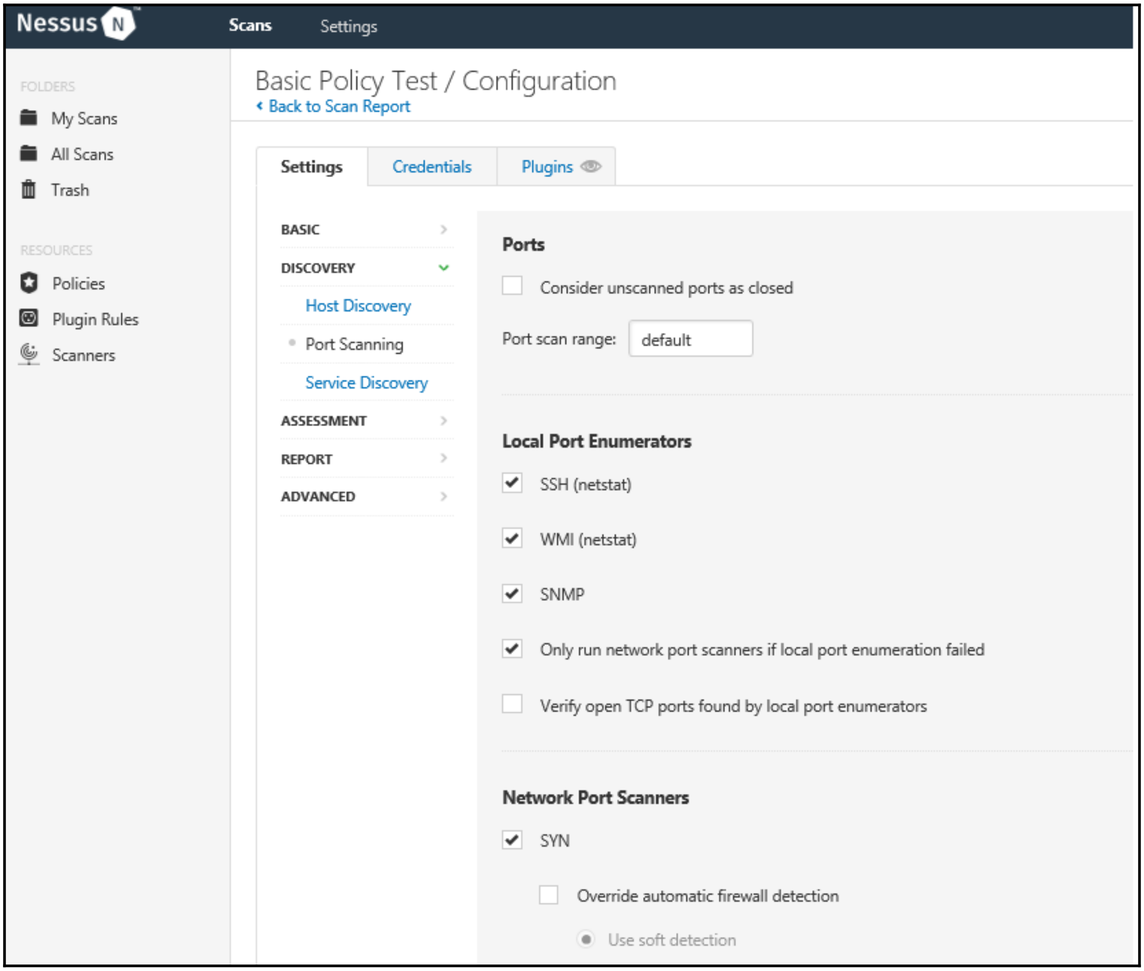
Destination ports: built-in

☑ ICMP

☐ Assume ICMP unreachable from the gateway means the host is down

Maximum number of retries: 2

☐ UDP



Basic Policy Test / Configuration

‹ Back to Scan Report

Ports

□ Consider unscanned ports as closed

Port scan range: default

Local Port Enumerators

☑ SSH (netstat)

☑ WMI (netstat)

☑ SNMP

☑ Only run network port scanners if local port enumeration failed

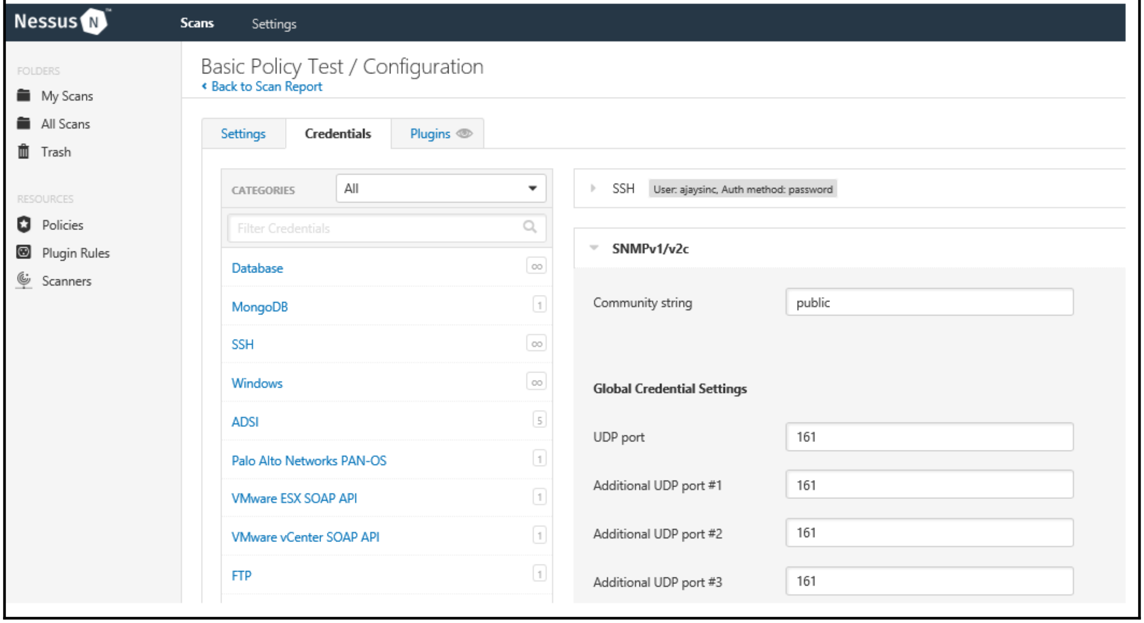
□ Verify open TCP ports found by local port enumerators

Network Port Scanners

☑ SYN

□ Override automatic firewall detection

● Use soft detection



Basic Policy Test / Configuration

CATEGORIES: All

Database	∞
MongoDB	1
SSH	∞
Windows	∞
ADSI	5
Palo Alto Networks PAN-OS	1
VMware ESX SOAP API	1
VMware vCenter SOAP API	1
FTP	1

SSH User: ajaysinc, Auth method: password

SNMPv1/v2c

Community string: public

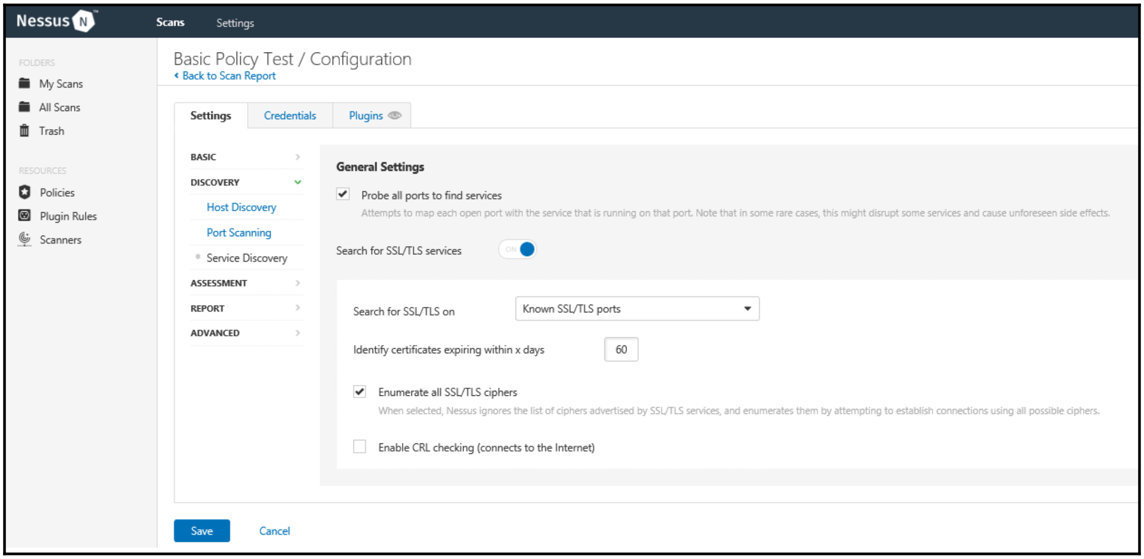
Global Credential Settings

UDP port: 161

Additional UDP port #1: 161

Additional UDP port #2: 161

Additional UDP port #3: 161



Basic Policy Test / Configuration

General Settings

☑ Probe all ports to find services

Attempts to map each open port with the service that is running on that port. Note that in some rare cases, this might disrupt some services and cause unforeseen side effects.

Search for SSL/TLS services: ON

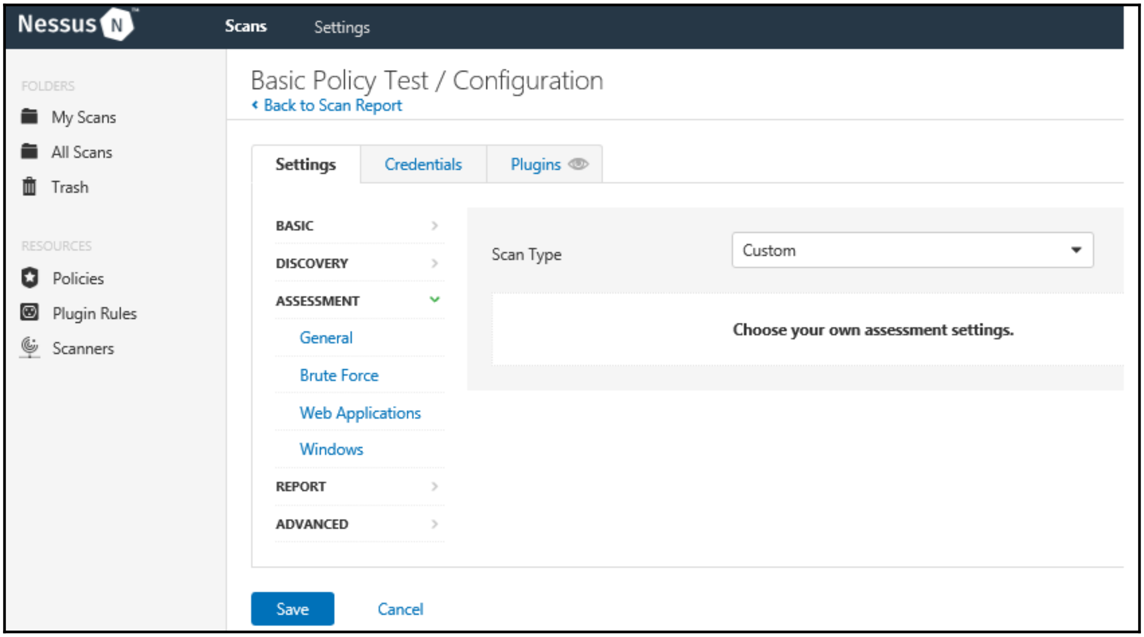
Search for SSL/TLS on: Known SSL/TLS ports

Identify certificates expiring within x days: 60

☑ Enumerate all SSL/TLS ciphers

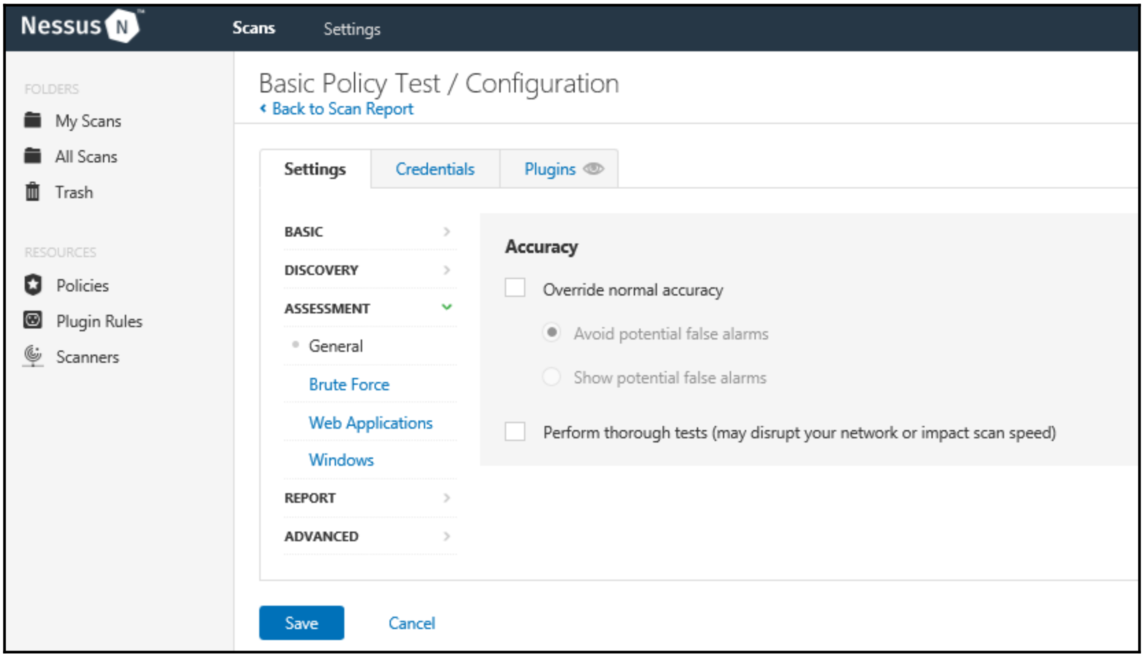
When selected, Nessus ignores the list of ciphers advertised by SSL/TLS services, and enumerates them by attempting to establish connections using all possible ciphers.

☐ Enable CRL checking (connects to the Internet)



Scan Type: Custom

Choose your own assessment settings.



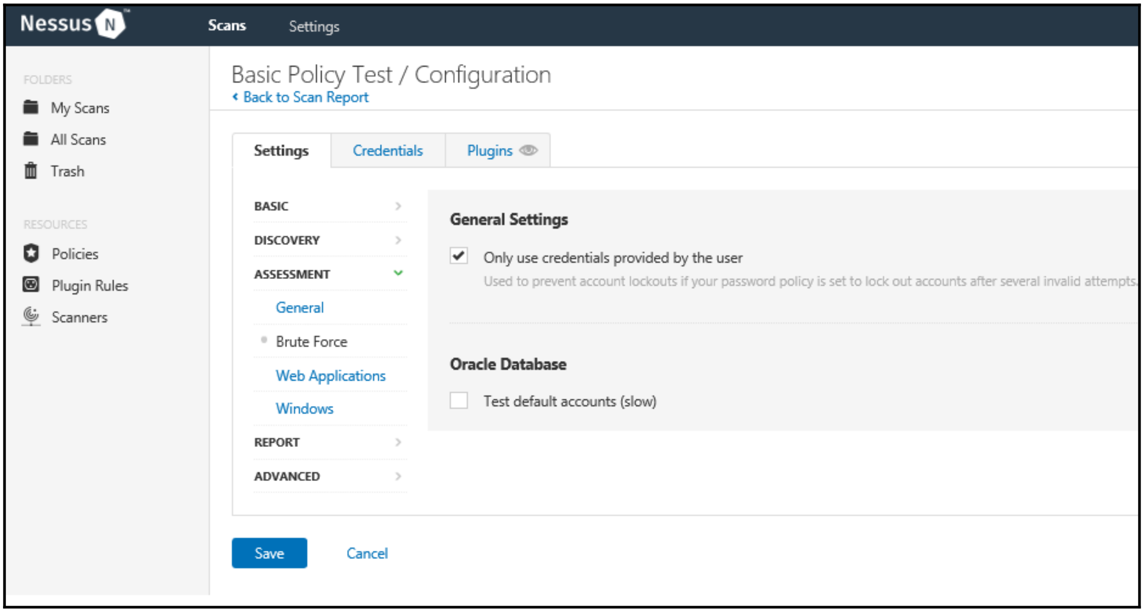
Accuracy

□ Override normal accuracy

● Avoid potential false alarms

○ Show potential false alarms

□ Perform thorough tests (may disrupt your network or impact scan speed)



Basic Policy Test / Configuration

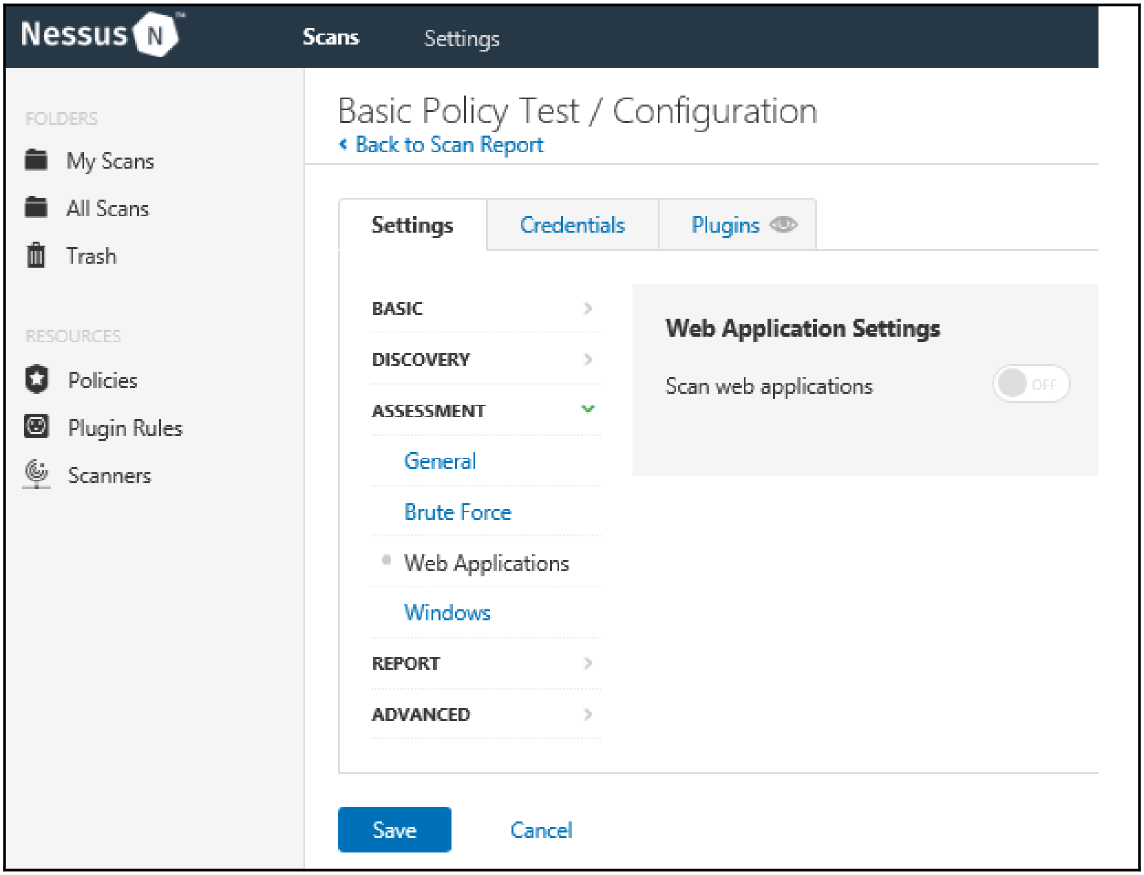
General Settings

☑ Only use credentials provided by the user

Used to prevent account lockouts if your password policy is set to lock out accounts after several invalid attempts.

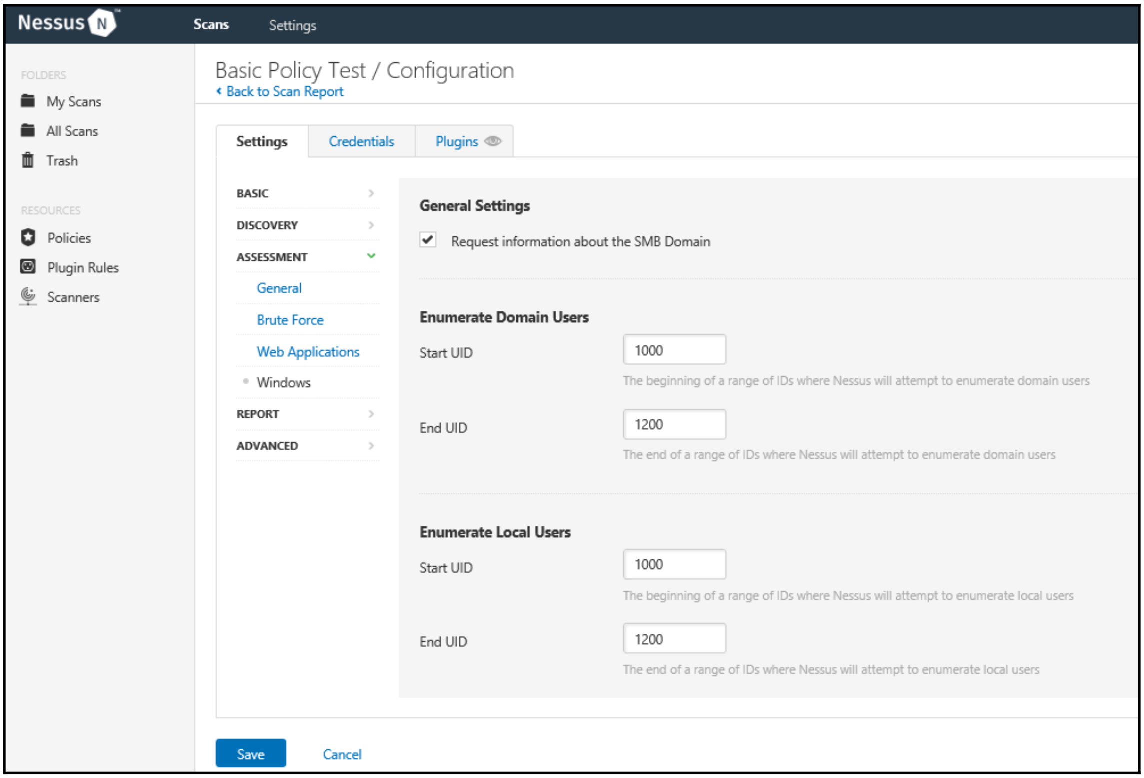
Oracle Database

□ Test default accounts (slow)



Web Application Settings

Scan web applications OFF



Basic Policy Test / Configuration

General Settings

☑ Request information about the SMB Domain

Enumerate Domain Users

Start UID: 1000

The beginning of a range of IDs where Nessus will attempt to enumerate domain users

End UID: 1200

The end of a range of IDs where Nessus will attempt to enumerate domain users

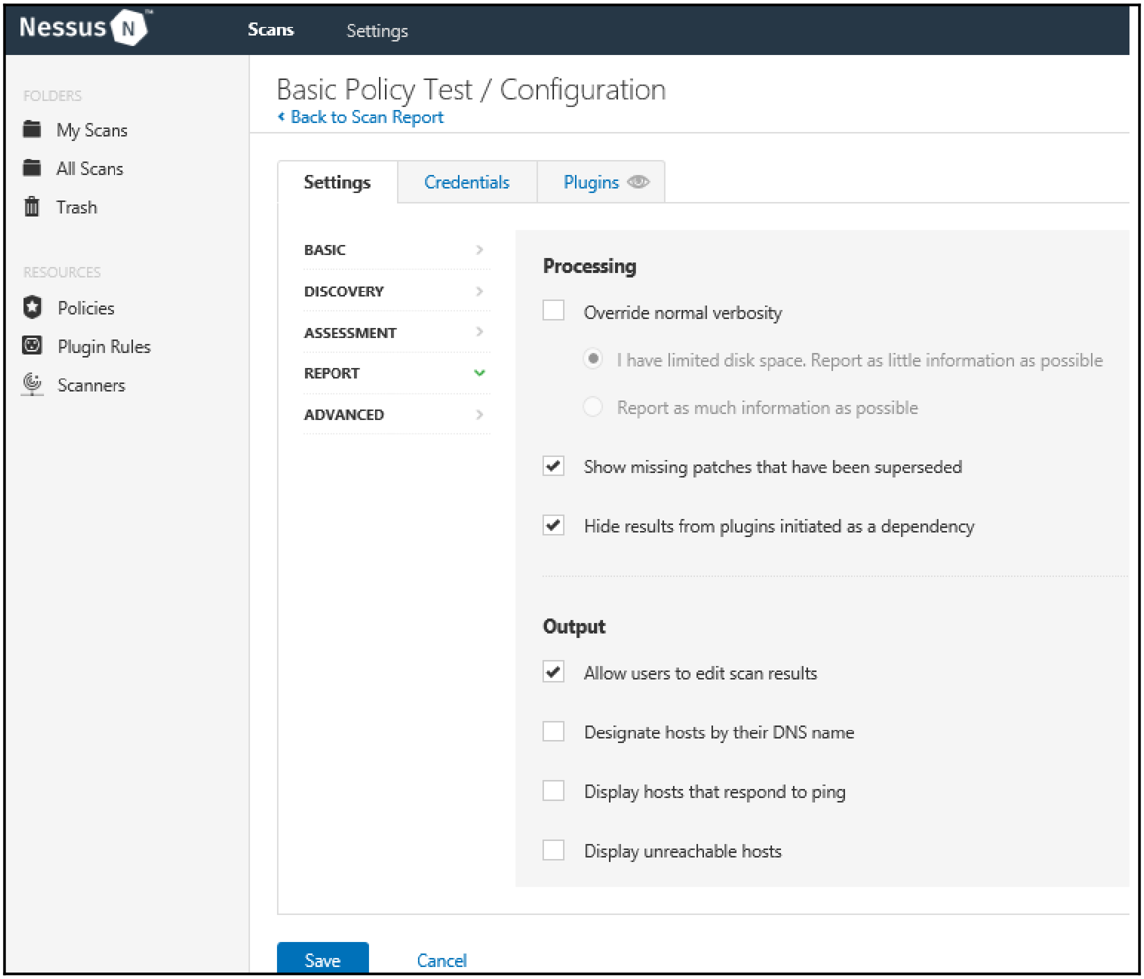
Enumerate Local Users

Start UID: 1000

The beginning of a range of IDs where Nessus will attempt to enumerate local users

End UID: 1200

The end of a range of IDs where Nessus will attempt to enumerate local users



Basic Policy Test / Configuration

Processing

□ Override normal verbosity

● I have limited disk space. Report as little information as possible

○ Report as much information as possible

☑ Show missing patches that have been superseded

☑ Hide results from plugins initiated as a dependency

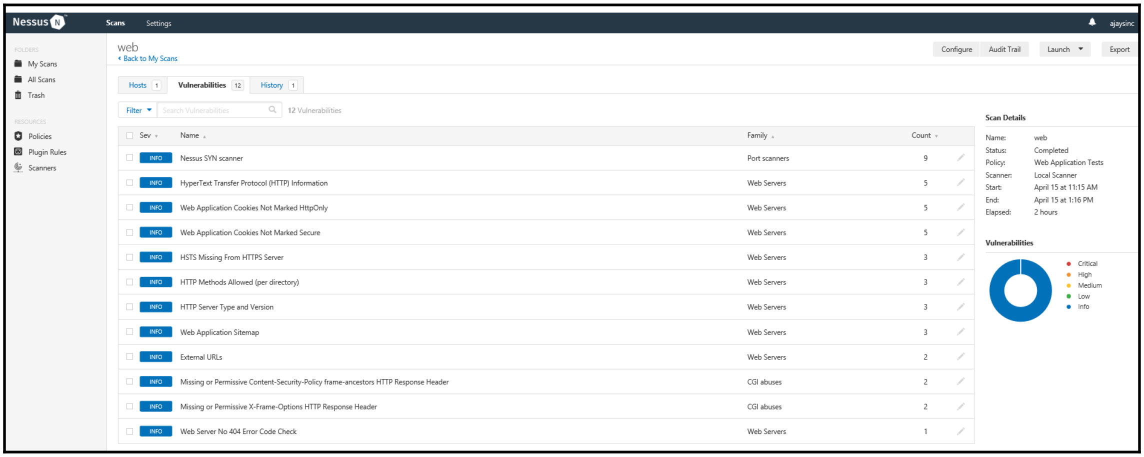
Output

☑ Allow users to edit scan results

□ Designate hosts by their DNS name

□ Display hosts that respond to ping

□ Display unreachable hosts



web
‹ Back to My Scans

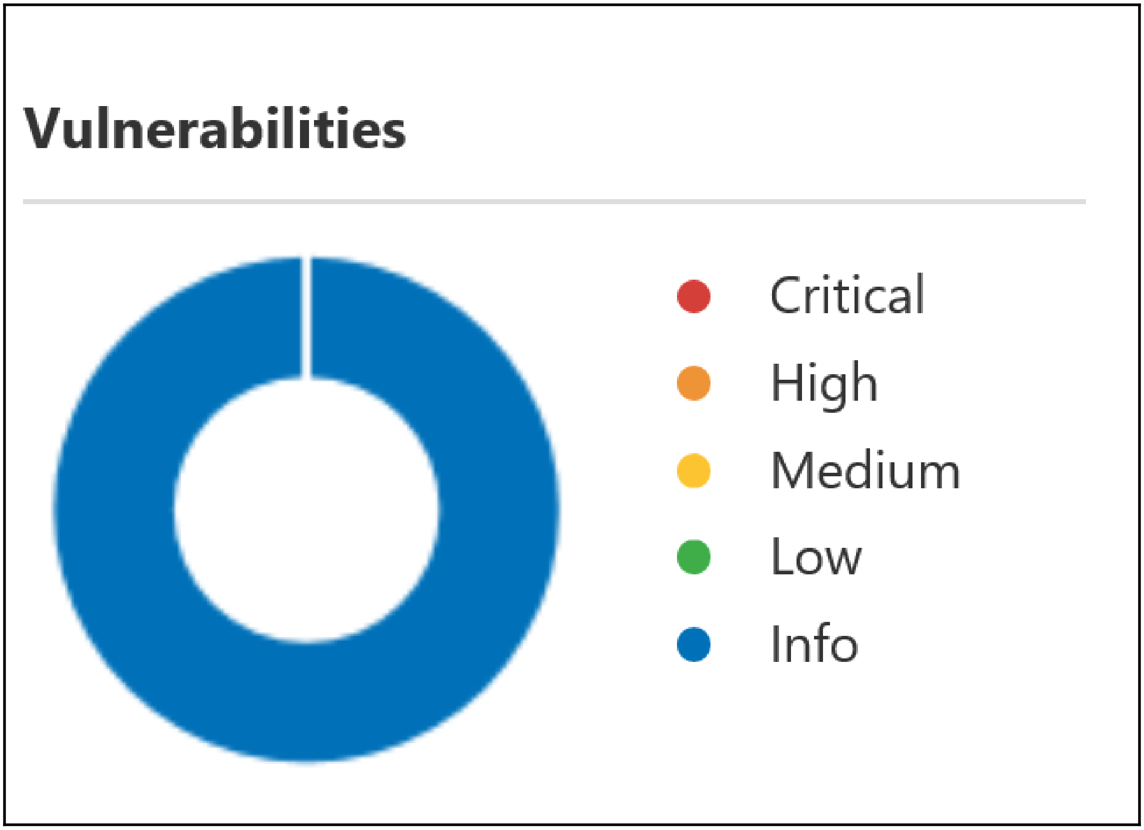
12 Vulnerabilities

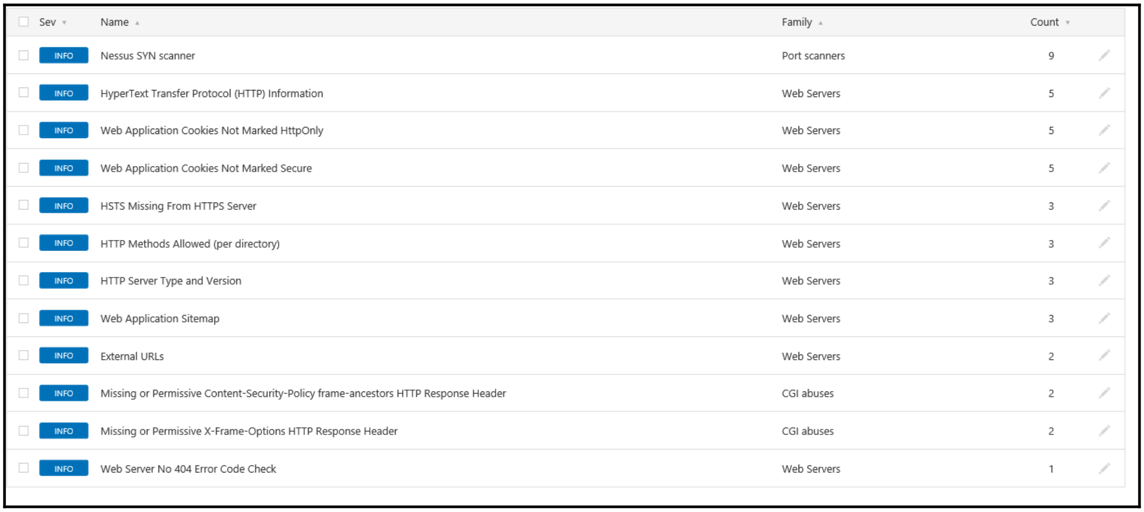
□	Sev	Name	Family	Count
□	INFO	Nessus SYN scanner	Port scanners	9
□	INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	5
□	INFO	Web Application Cookies Not Marked HttpOnly	Web Servers	5
□	INFO	Web Application Cookies Not Marked Secure	Web Servers	5
□	INFO	HSTS Missing From HTTPS Server	Web Servers	3
□	INFO	HTTP Methods Allowed (per directory)	Web Servers	3
□	INFO	HTTP Server Type and Version	Web Servers	3
□	INFO	Web Application Sitemap	Web Servers	3
□	INFO	External URLs	Web Servers	2
□	INFO	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	CGI abuses	2
□	INFO	Missing or Permissive X-Frame-Options HTTP Response Header	CGI abuses	2
□	INFO	Web Server No 404 Error Code Check	Web Servers	1

Scan Details

Name:	web
Status:	Completed
Policy:	Web Application Tests
Scanner:	Local Scanner
Start:	April 15 at 11:15 AM
End:	April 15 at 1:16 PM
Elapsed:	2 hours

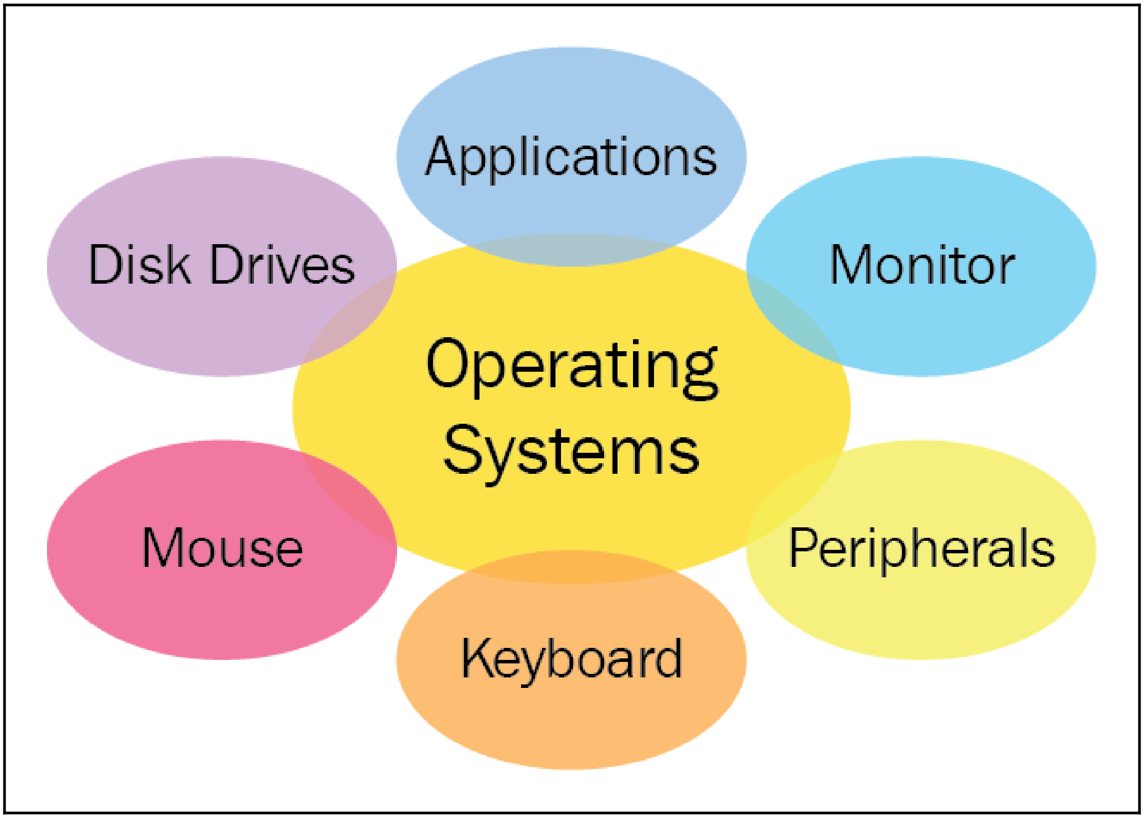
Vulnerabilities

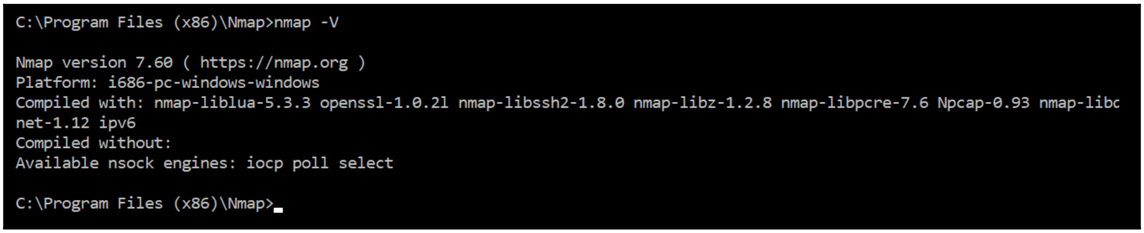




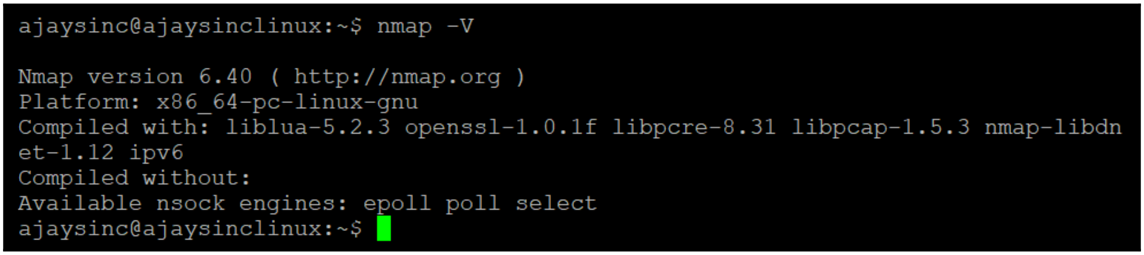
□	Sev	Name	Family	Count
□	INFO	Nessus SYN scanner	Port scanners	9
□	INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	5
□	INFO	Web Application Cookies Not Marked HttpOnly	Web Servers	5
□	INFO	Web Application Cookies Not Marked Secure	Web Servers	5
□	INFO	HSTS Missing From HTTPS Server	Web Servers	3
□	INFO	HTTP Methods Allowed (per directory)	Web Servers	3
□	INFO	HTTP Server Type and Version	Web Servers	3
□	INFO	Web Application Sitemap	Web Servers	3
□	INFO	External URLs	Web Servers	2
□	INFO	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	CGI abuses	2
□	INFO	Missing or Permissive X-Frame-Options HTTP Response Header	CGI abuses	2
□	INFO	Web Server No 404 Error Code Check	Web Servers	1

Chapter 8: Remote OS Detection

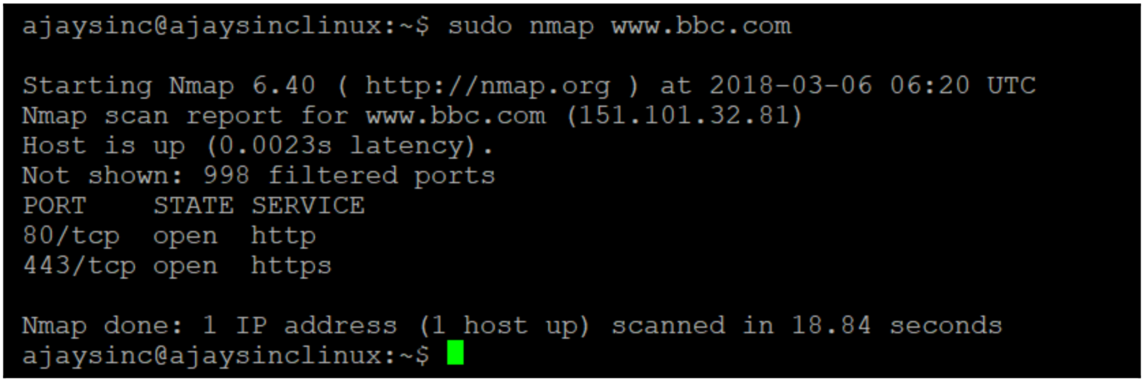




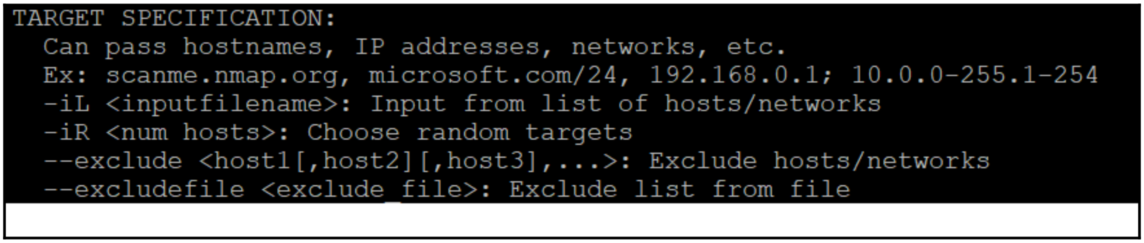
```
C:\Program Files (x86)\Nmap>nmap -V

Nmap version 7.60 ( https://nmap.org )
Platform: i686-pc-windows-windows
Compiled with: nmap-liblua-5.3.3 openssl-1.0.2l nmap-libssh2-1.8.0 nmap-libz-1.2.8 nmap-libpcre-7.6 Npcap-0.93 nmap-libc
net-1.12 ipv6
Compiled without:
Available nsock engines: iocp poll select

C:\Program Files (x86)\Nmap>_
```



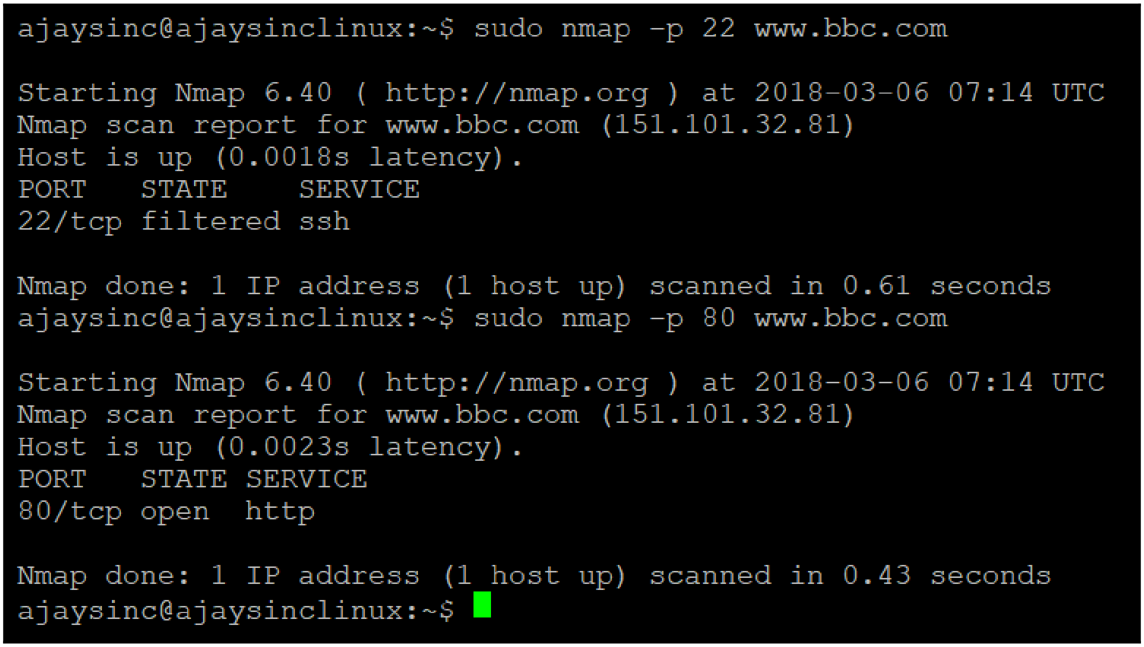
```
ajaysinc@ajaysinclinux:~$ nmap -V

Nmap version 6.40 ( http://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.2.3 openssl-1.0.1f libpcre-8.31 libpcap-1.5.3 nmap-libdn
et-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
ajaysinc@ajaysinclinux:~$
```



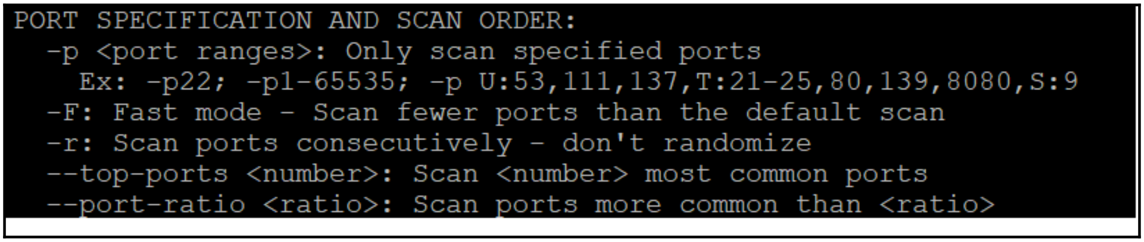
```
ajaysinc@ajaysinclinux:~$ sudo nmap www.bbc.com

Starting Nmap 6.40 ( http://nmap.org ) at 2018-03-06 06:20 UTC
Nmap scan report for www.bbc.com (151.101.32.81)
Host is up (0.0023s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 18.84 seconds
ajaysinc@ajaysinclinux:~$
```



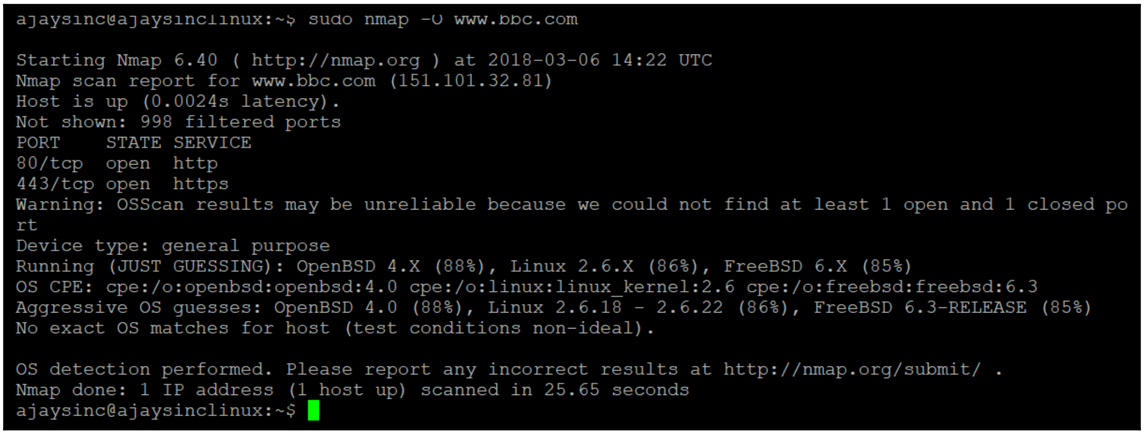
```
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
```



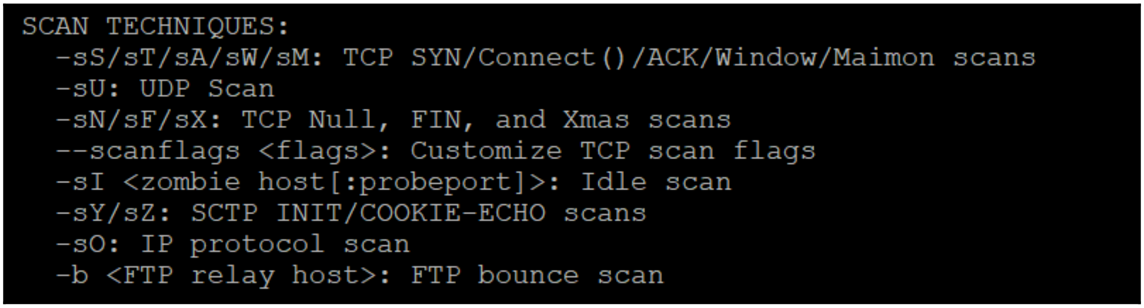
```
ajaysinc@ajaysinclinux:~$ sudo nmap -p 22 www.bbc.com

Starting Nmap 6.40 ( http://nmap.org ) at 2018-03-06 07:14 UTC
Nmap scan report for www.bbc.com (151.101.32.81)
Host is up (0.0018s latency).
PORT   STATE    SERVICE
22/tcp filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
ajaysinc@ajaysinclinux:~$ sudo nmap -p 80 www.bbc.com

Starting Nmap 6.40 ( http://nmap.org ) at 2018-03-06 07:14 UTC
Nmap scan report for www.bbc.com (151.101.32.81)
Host is up (0.0023s latency).
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
ajaysinc@ajaysinclinux:~$ 
```



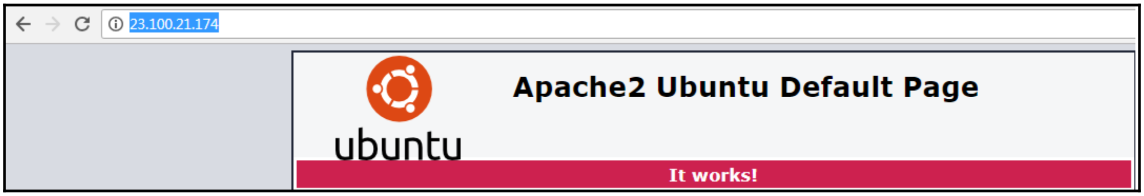
```
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
```



```
ajaysinc@ajaysinclinux:~$ sudo nmap -O www.bbc.com

Starting Nmap 6.40 ( http://nmap.org ) at 2018-03-06 14:22 UTC
Nmap scan report for www.bbc.com (151.101.32.81)
Host is up (0.0024s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed po
rt
Device type: general purpose
Running (JUST GUESSING): OpenBSD 4.X (88%), Linux 2.6.X (86%), FreeBSD 6.X (85%)
OS CPE: cpe:/o:openbsd:openbsd:4.0 cpe:/o:linux:linux_kernel:2.6 cpe:/o:freebsd:freebsd:6.3
Aggressive OS guesses: OpenBSD 4.0 (88%), Linux 2.6.18 - 2.6.22 (86%), FreeBSD 6.3-RELEASE (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.65 seconds
ajaysinc@ajaysinclinux:~$ 
```

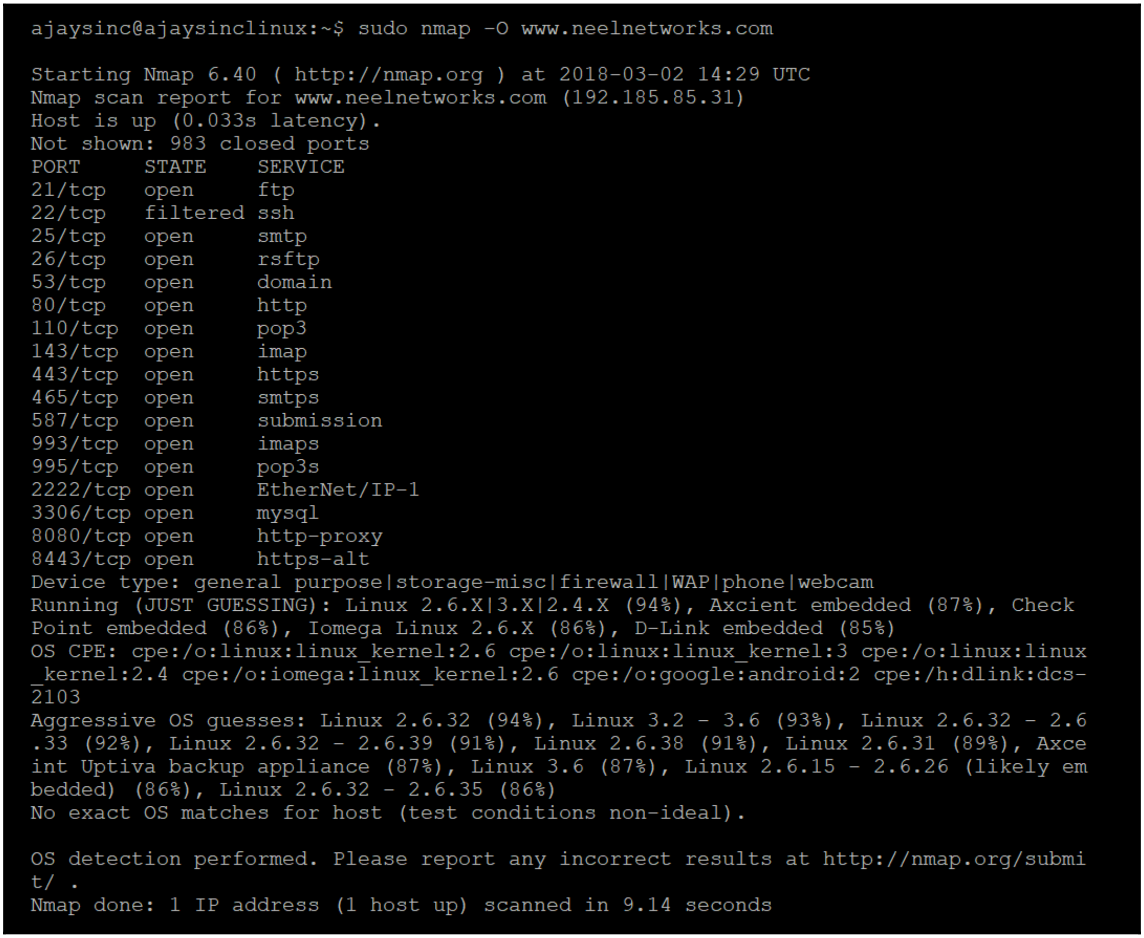


```
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
```

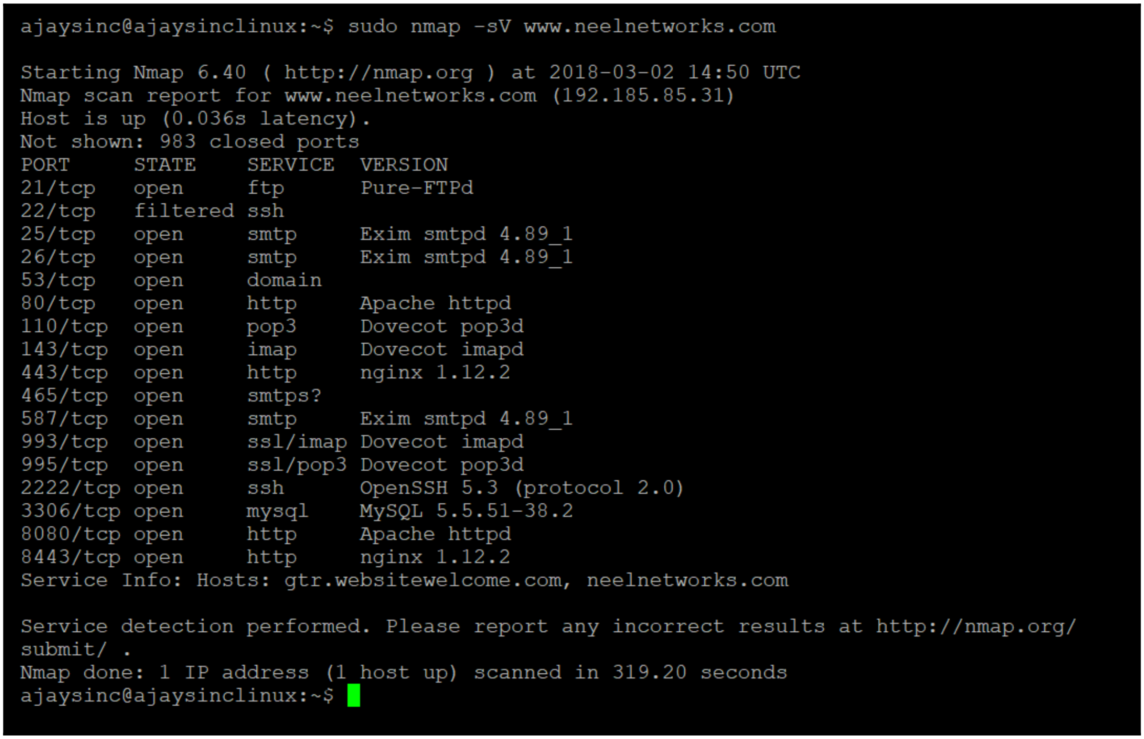


Apache2 Ubuntu Default Page

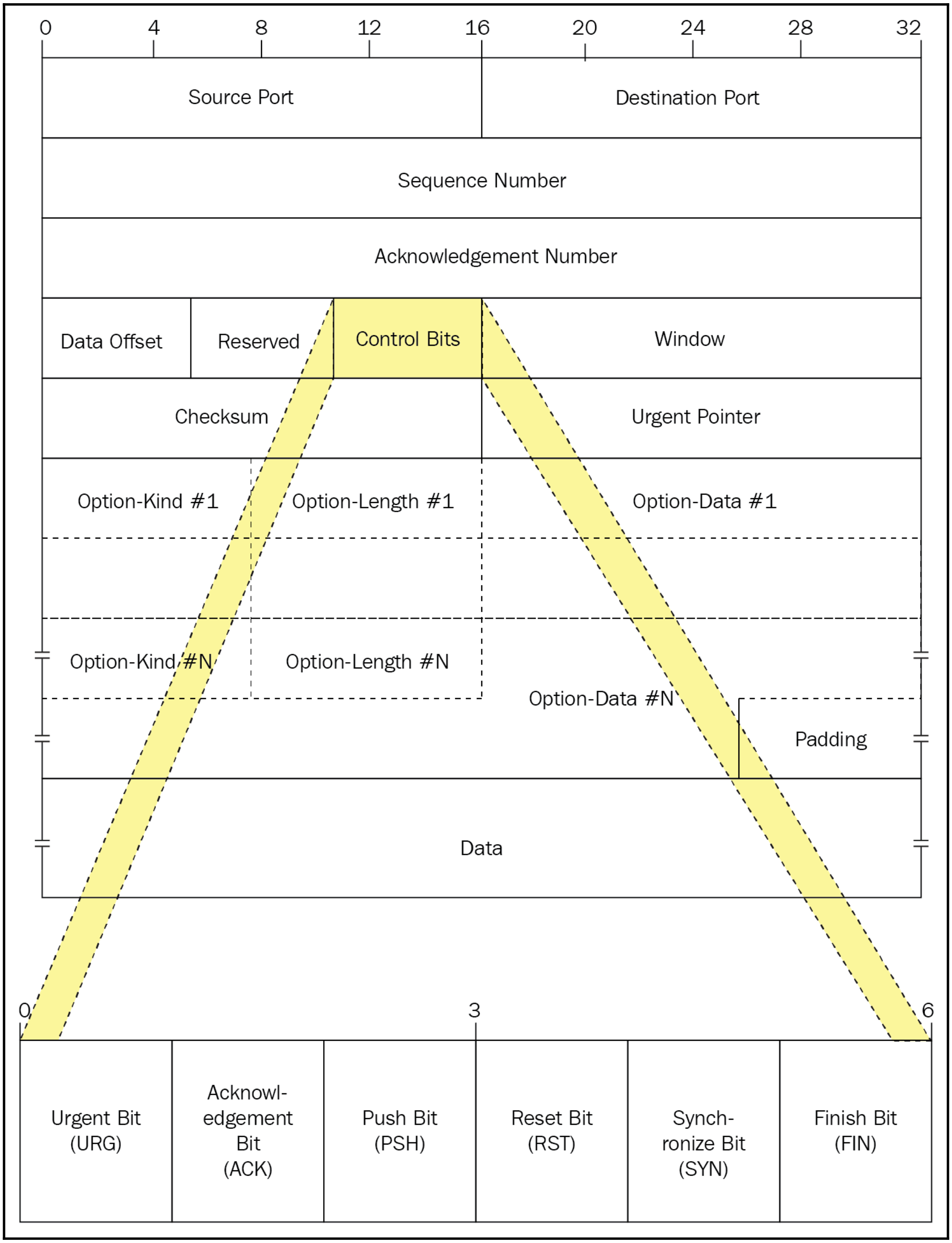
It works!

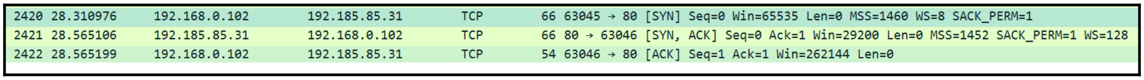


```
ajaysinc@ajaysinclinux:~$ sudo nmap -O www.neelnetworks.com

Starting Nmap 6.40 ( http://nmap.org ) at 2018-03-02 14:29 UTC
Nmap scan report for www.neelnetworks.com (192.185.85.31)
Host is up (0.033s latency).
Not shown: 983 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
25/tcp   open     smtp
26/tcp   open     rsftp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
143/tcp  open     imap
443/tcp  open     https
465/tcp  open     smtps
587/tcp  open     submission
993/tcp  open     imaps
995/tcp  open     pop3s
2222/tcp open     EtherNet/IP-1
3306/tcp open     mysql
8080/tcp open     http-proxy
8443/tcp open     https-alt
Device type: general purpose|storage-misc|firewall|WAP|phone|webcam
Running (JUST GUESSING): Linux 2.6.X|3.X|2.4.X (94%), Axcient embedded (87%), Check
Point embedded (86%), Iomega Linux 2.6.X (86%), D-Link embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux
_kernel:2.4 cpe:/o:iomega:linux_kernel:2.6 cpe:/o:google:android:2 cpe:/h:dlink:dcs-
2103
Aggressive OS guesses: Linux 2.6.32 (94%), Linux 3.2 - 3.6 (93%), Linux 2.6.32 - 2.6
.33 (92%), Linux 2.6.32 - 2.6.39 (91%), Linux 2.6.38 (91%), Linux 2.6.31 (89%), Axce
int Uptiva backup appliance (87%), Linux 3.6 (87%), Linux 2.6.15 - 2.6.26 (likely em
bedded) (86%), Linux 2.6.32 - 2.6.35 (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 9.14 seconds
```

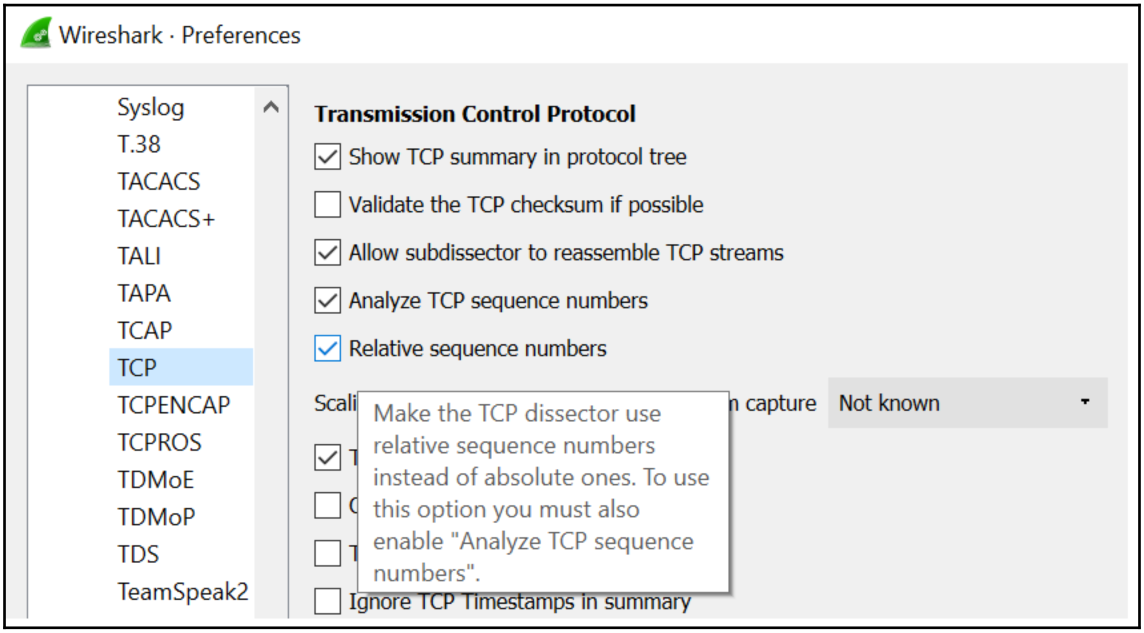


```
ajaysinc@ajaysinclinux:~$ sudo nmap -sV www.neelnetworks.com

Starting Nmap 6.40 ( http://nmap.org ) at 2018-03-02 14:50 UTC
Nmap scan report for www.neelnetworks.com (192.185.85.31)
Host is up (0.036s latency).
Not shown: 983 closed ports
PORT     STATE    SERVICE  VERSION
21/tcp   open     ftp      Pure-FTPd
22/tcp   filtered ssh
25/tcp   open     smtp     Exim smtpd 4.89_1
26/tcp   open     smtp     Exim smtpd 4.89_1
53/tcp   open     domain
80/tcp   open     http     Apache httpd
110/tcp  open     pop3     Dovecot pop3d
143/tcp  open     imap     Dovecot imapd
443/tcp  open     http     nginx 1.12.2
465/tcp  open     smtps?
587/tcp  open     smtp     Exim smtpd 4.89_1
993/tcp  open     ssl/imap Dovecot imapd
995/tcp  open     ssl/pop3 Dovecot pop3d
2222/tcp open     ssh      OpenSSH 5.3 (protocol 2.0)
3306/tcp open     mysql    MySQL 5.5.51-38.2
8080/tcp open     http     Apache httpd
8443/tcp open     http     nginx 1.12.2
Service Info: Hosts: gtr.websitewelcome.com, neelnetworks.com

Service detection performed. Please report any incorrect results at http://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 319.20 seconds
ajaysinc@ajaysinclinux:~$ 
```


0
4
8
12
16
20
24
28
32
Source Port
Destination Port
Sequence Number
Acknowledgement Number
Data Offset
Reserved
Control Bits
Window
Checksum
Urgent Pointer
Option-Kind #1
Option-Length #1
Option-Data #1
Option-Kind #N
Option-Length #N
Option-Data #N
Padding
Data
0
3
6
Urgent Bit (URG)
Acknowl-edgement Bit (ACK)
Push Bit (PSH)
Reset Bit (RST)
Synch-ronize Bit (SYN)
Finish Bit (FIN)



```
2420 28.310976   192.168.0.102   192.185.85.31   TCP   66 63045 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
2421 28.565106   192.185.85.31   192.168.0.102   TCP   66 80 → 63046 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM=1 WS=128
2422 28.565199   192.168.0.102   192.185.85.31   TCP   54 63046 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
```



Wireshark · Preferences

Transmission Control Protocol

☑ Show TCP summary in protocol tree

□ Validate the TCP checksum if possible

☑ Allow subdissector to reassemble TCP streams

☑ Analyze TCP sequence numbers

☑ Relative sequence numbers

Scali n capture Not known

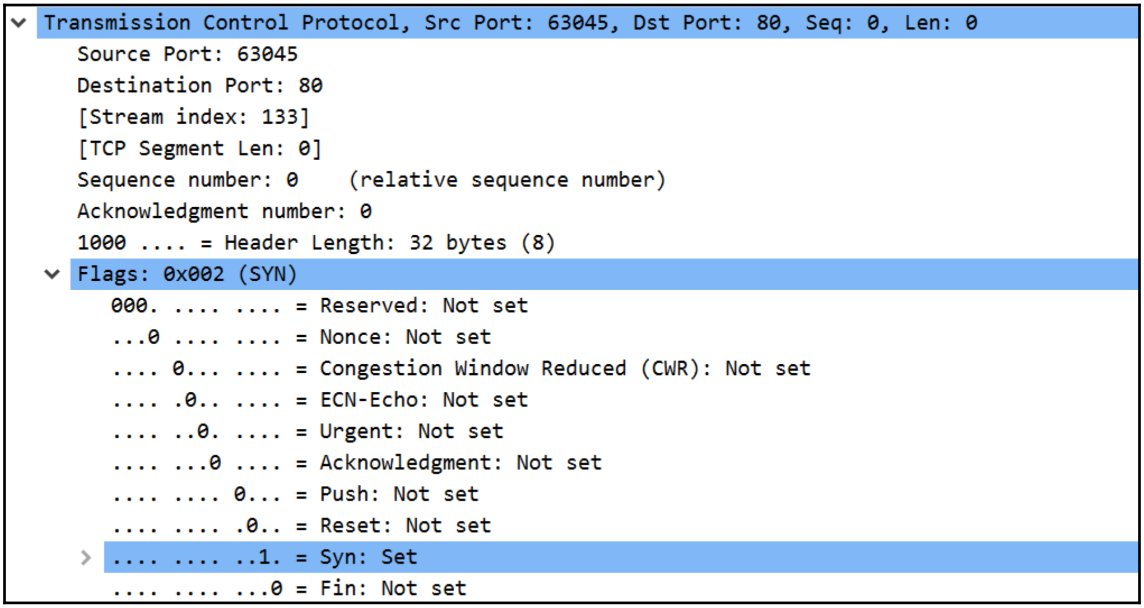
☑ T

□ C

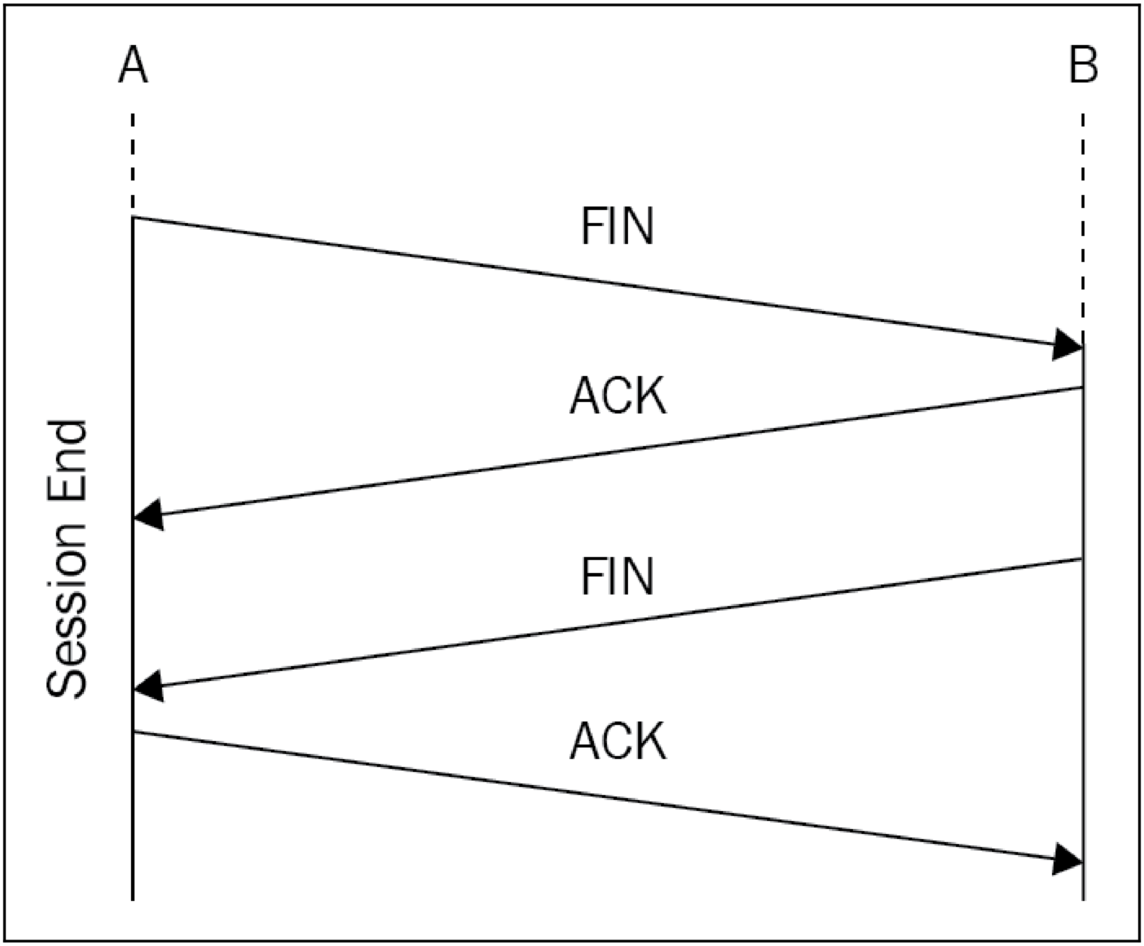
□ T

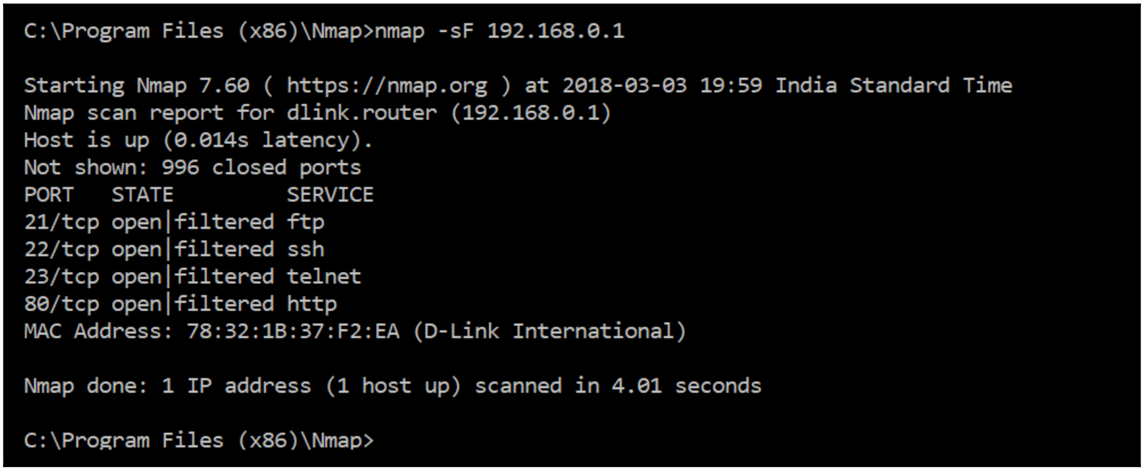
□ Ignore TCP Timestamps in summary

Make the TCP dissector use relative sequence numbers instead of absolute ones. To use this option you must also enable "Analyze TCP sequence numbers".

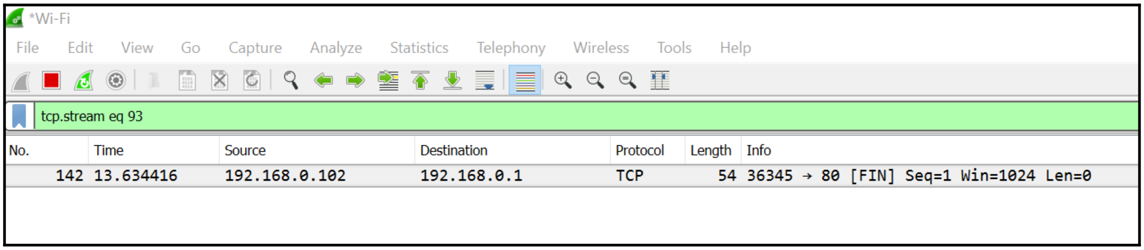


```
Transmission Control Protocol, Src Port: 63045, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 63045
    Destination Port: 80
    [Stream index: 133]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    1000 .... = Header Length: 32 bytes (8)
  Flags: 0x002 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgment: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
```


A
B
FIN
ACK
FIN
ACK
Session End

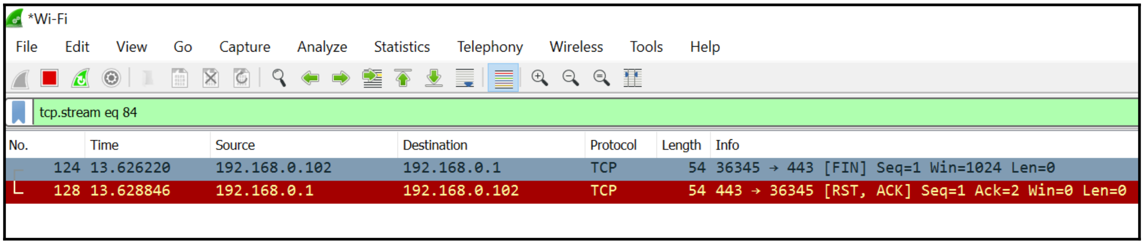


```
C:\Program Files (x86)\Nmap>nmap -sF 192.168.0.1

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-03 19:59 India Standard Time
Nmap scan report for dlink.router (192.168.0.1)
Host is up (0.014s latency).
Not shown: 996 closed ports
PORT   STATE         SERVICE
21/tcp open|filtered ftp
22/tcp open|filtered ssh
23/tcp open|filtered telnet
80/tcp open|filtered http
MAC Address: 78:32:1B:37:F2:EA (D-Link International)

Nmap done: 1 IP address (1 host up) scanned in 4.01 seconds

C:\Program Files (x86)\Nmap>
```



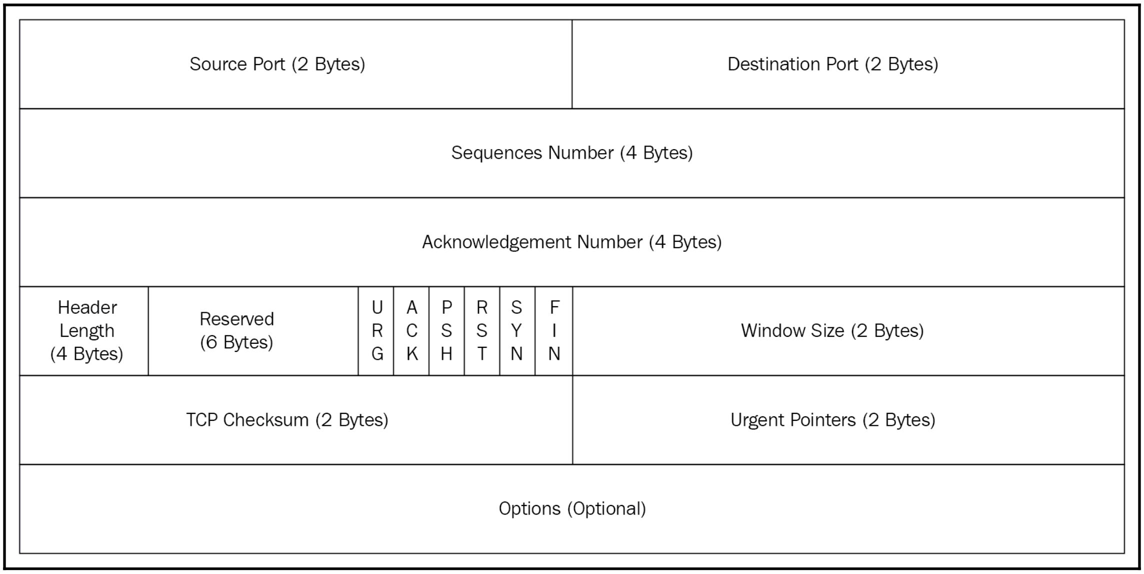
tcp.stream eq 93

No.	Time	Source	Destination	Protocol	Length	Info
142	13.634416	192.168.0.102	192.168.0.1	TCP	54	36345 → 80 [FIN] Seq=1 Win=1024 Len=0

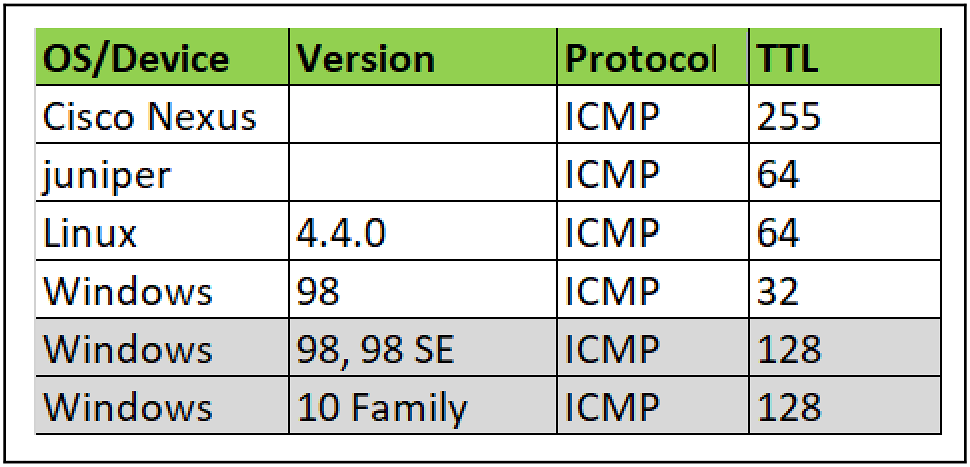


tcp.stream eq 84

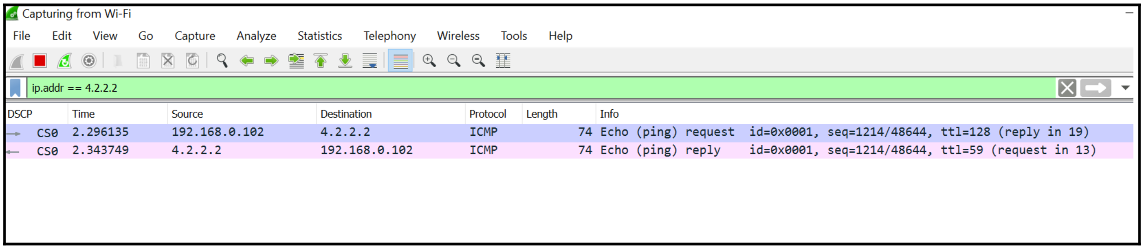
No.	Time	Source	Destination	Protocol	Length	Info
124	13.626220	192.168.0.102	192.168.0.1	TCP	54	36345 → 443 [FIN] Seq=1 Win=1024 Len=0
128	13.628846	192.168.0.1	192.168.0.102	TCP	54	443 → 36345 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0



<table>
<tr><td colspan="8">Source Port (2 Bytes)</td><td>Destination Port (2 Bytes)</td></tr>
<tr><td colspan="9">Sequences Number (4 Bytes)</td></tr>
<tr><td colspan="9">Acknowledgement Number (4 Bytes)</td></tr>
<tr><td>Header Length (4 Bytes)</td><td>Reserved (6 Bytes)</td><td>U R G</td><td>A C K</td><td>P S H</td><td>R S T</td><td>S Y N</td><td>F I N</td><td>Window Size (2 Bytes)</td></tr>
<tr><td colspan="8">TCP Checksum (2 Bytes)</td><td>Urgent Pointers (2 Bytes)</td></tr>
<tr><td colspan="9">Options (Optional)</td></tr>
</table>

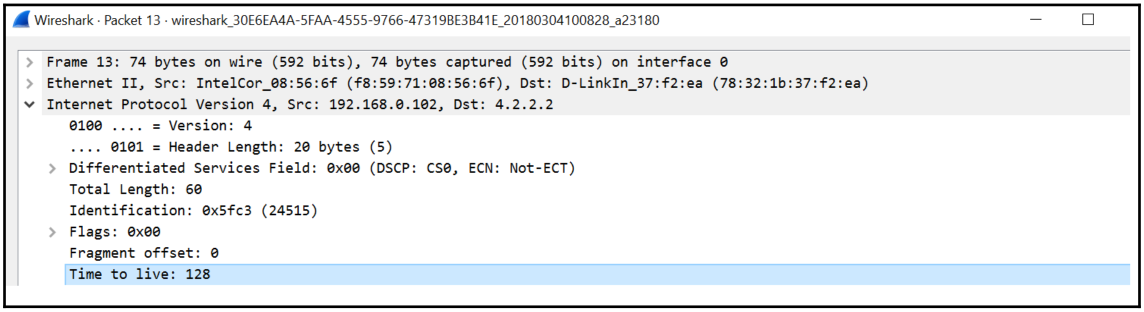


OS/Device	Version	Protocol	TTL
Cisco Nexus		ICMP	255
juniper		ICMP	64
Linux	4.4.0	ICMP	64
Windows	98	ICMP	32
Windows	98, 98 SE	ICMP	128
Windows	10 Family	ICMP	128



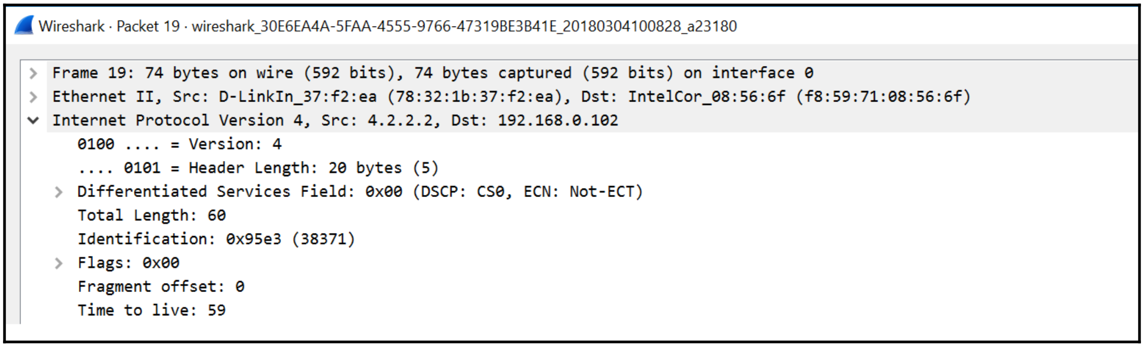
ip.addr == 4.2.2.2

```
DSCP  Time      Source         Destination    Protocol  Length  Info
CS0   2.296135  192.168.0.102  4.2.2.2        ICMP          74  Echo (ping) request  id=0x0001, seq=1214/48644, ttl=128 (reply in 19)
CS0   2.343749  4.2.2.2        192.168.0.102  ICMP          74  Echo (ping) reply    id=0x0001, seq=1214/48644, ttl=59 (request in 13)
```



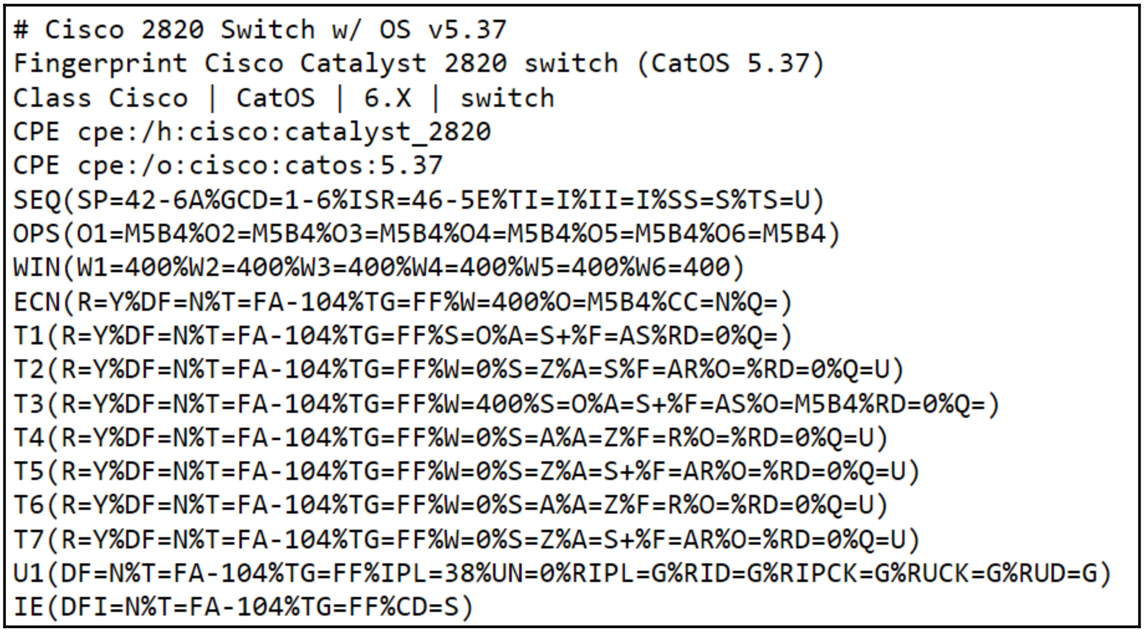
Wireshark · Packet 13 · wireshark_30E6EA4A-5FAA-4555-9766-47319BE3B41E_20180304100828_a23180

```
> Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: IntelCor_08:56:6f (f8:59:71:08:56:6f), Dst: D-LinkIn_37:f2:ea (78:32:1b:37:f2:ea)
v Internet Protocol Version 4, Src: 192.168.0.102, Dst: 4.2.2.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x5fc3 (24515)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 128
```



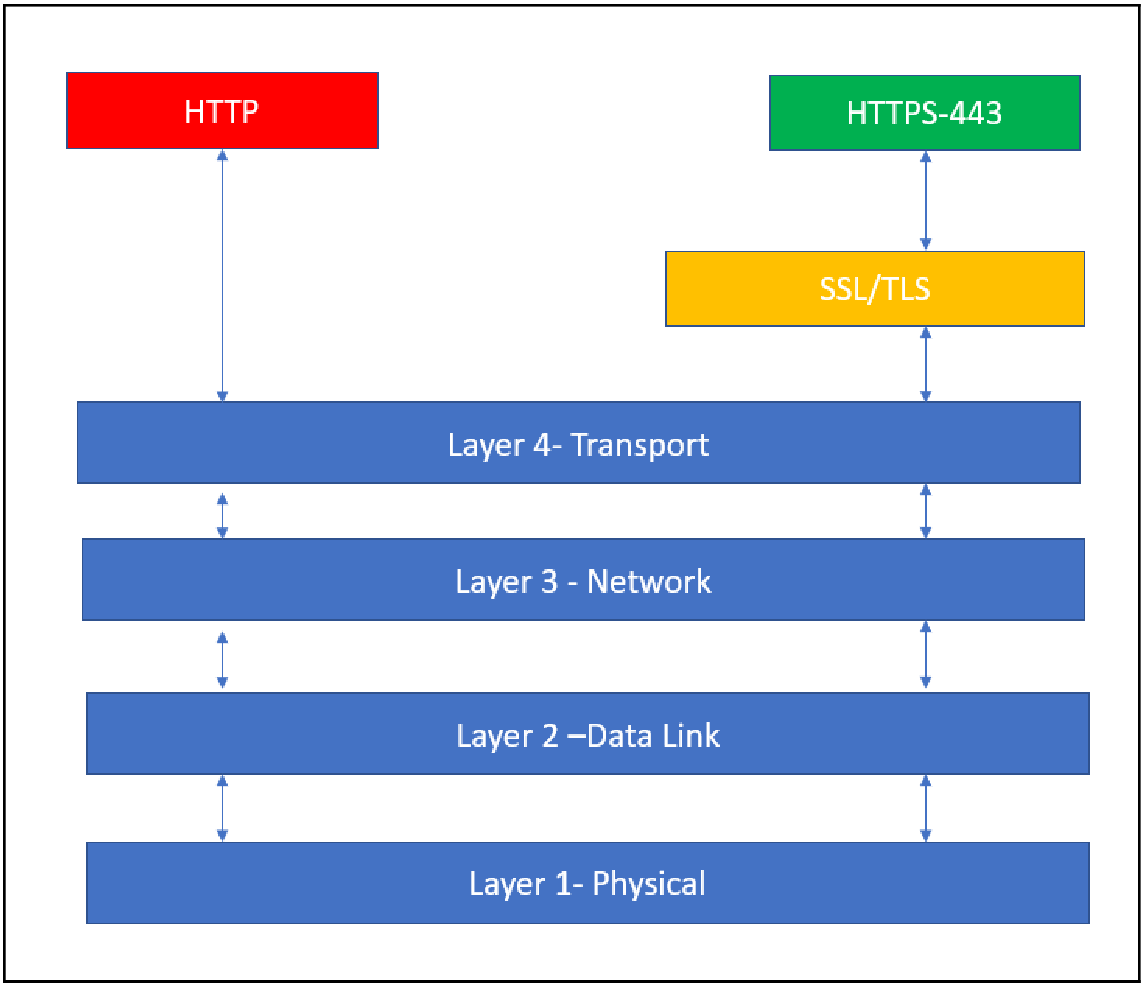
Wireshark · Packet 19 · wireshark_30E6EA4A-5FAA-4555-9766-47319BE3B41E_20180304100828_a23180

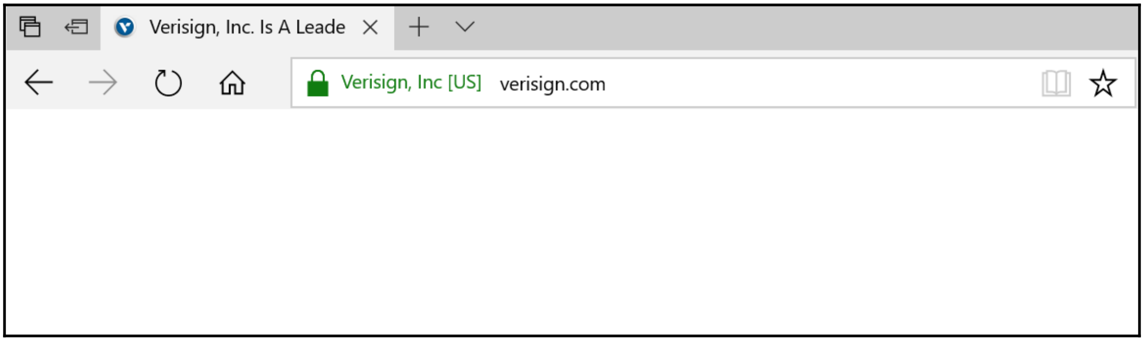
```
> Frame 19: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: D-LinkIn_37:f2:ea (78:32:1b:37:f2:ea), Dst: IntelCor_08:56:6f (f8:59:71:08:56:6f)
v Internet Protocol Version 4, Src: 4.2.2.2, Dst: 192.168.0.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x95e3 (38371)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 59
```

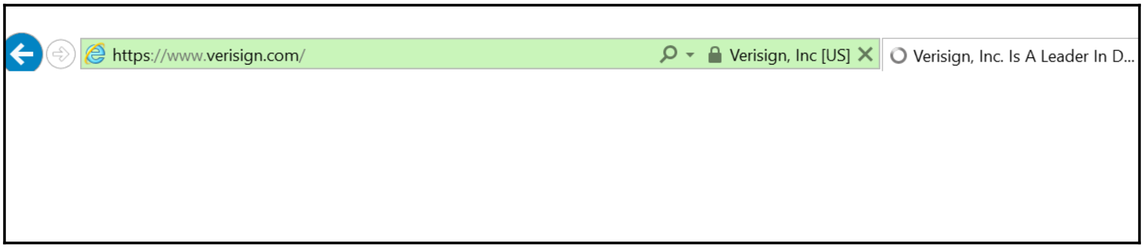


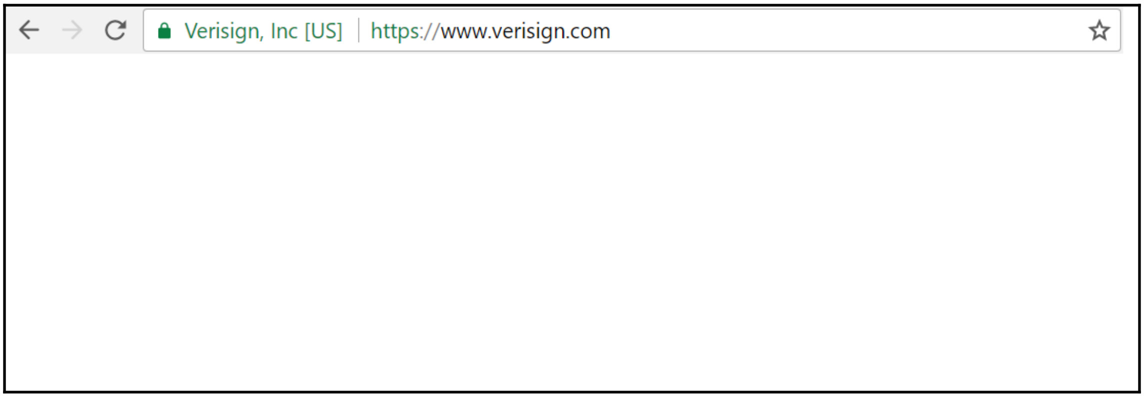
```
# Cisco 2820 Switch w/ OS v5.37
Fingerprint Cisco Catalyst 2820 switch (CatOS 5.37)
Class Cisco | CatOS | 6.X | switch
CPE cpe:/h:cisco:catalyst_2820
CPE cpe:/o:cisco:catos:5.37
SEQ(SP=42-6A%GCD=1-6%ISR=46-5E%TI=I%II=I%SS=S%TS=U)
OPS(O1=M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)
WIN(W1=400%W2=400%W3=400%W4=400%W5=400%W6=400)
ECN(R=Y%DF=N%T=FA-104%TG=FF%W=400%O=M5B4%CC=N%Q=)
T1(R=Y%DF=N%T=FA-104%TG=FF%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=Y%DF=N%T=FA-104%TG=FF%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=U)
T3(R=Y%DF=N%T=FA-104%TG=FF%W=400%S=O%A=S+%F=AS%O=M5B4%RD=0%Q=)
T4(R=Y%DF=N%T=FA-104%TG=FF%W=0%S=A%A=Z%F=R%O=%RD=0%Q=U)
T5(R=Y%DF=N%T=FA-104%TG=FF%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=U)
T6(R=Y%DF=N%T=FA-104%TG=FF%W=0%S=A%A=Z%F=R%O=%RD=0%Q=U)
T7(R=Y%DF=N%T=FA-104%TG=FF%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=U)
U1(DF=N%T=FA-104%TG=FF%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(DFI=N%T=FA-104%TG=FF%CD=S)
```

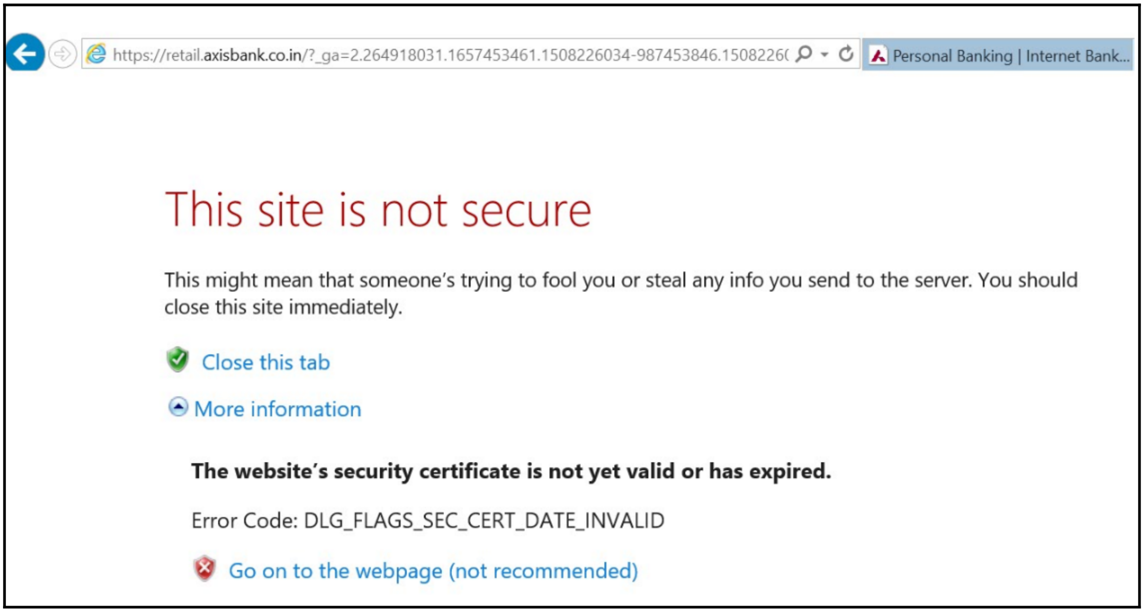
Chapter 9: Public key infrastructure –SSL




Verisign, Inc. Is A Leade
Verisign, Inc [US]
verisign.com


https://www.verisign.com/
Verisign, Inc [US]
Verisign, Inc. Is A Leader In D...


Verisign, Inc [US]
https://www.verisign.com



https://retail.axisbank.co.in/?_ga=2.264918031.1657453461.1508226034-987453846.1508226(
Personal Banking | Internet Bank...

This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

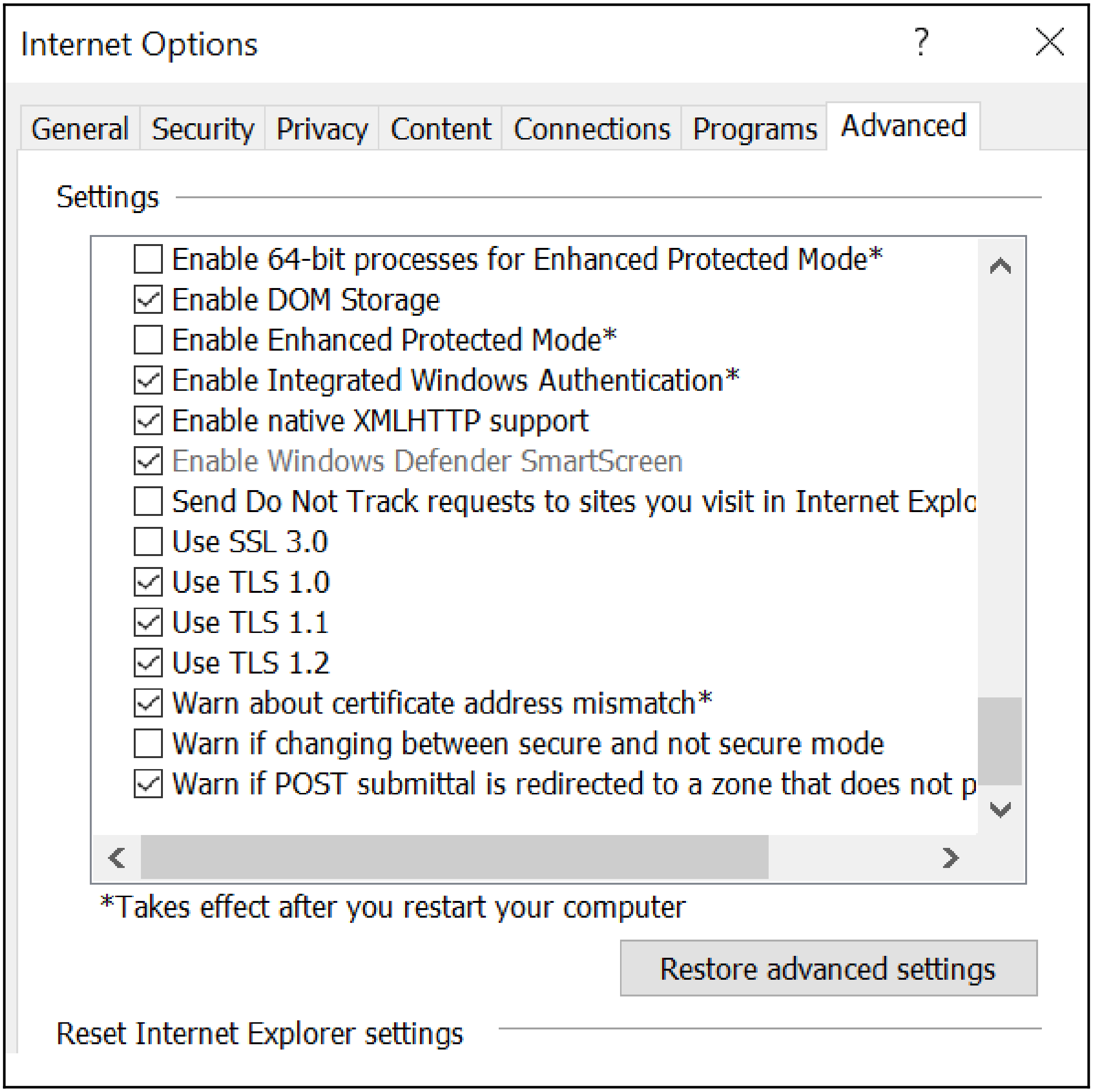
Close this tab

More information

The website's security certificate is not yet valid or has expired.

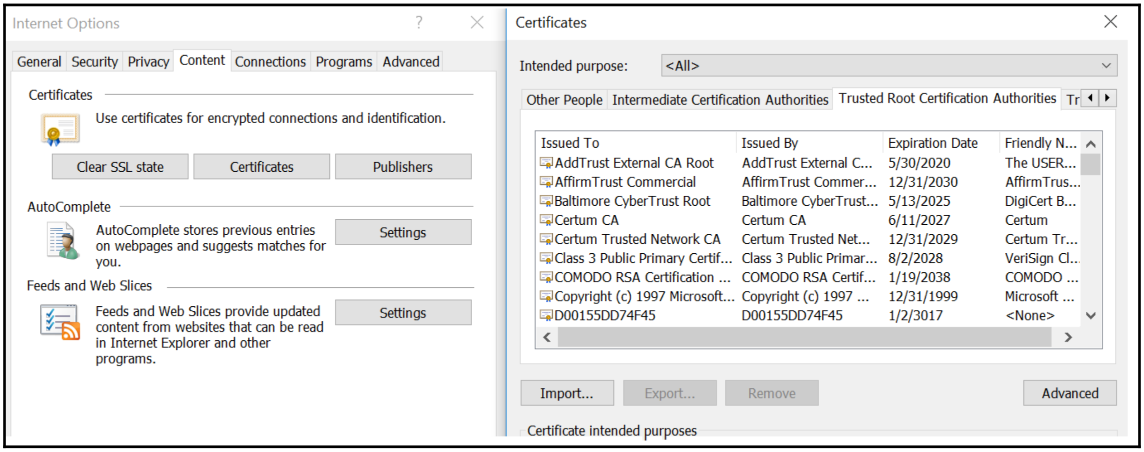
Error Code: DLG_FLAGS_SEC_CERT_DATE_INVALID

Go on to the webpage (not recommended)



☐ Enable 64-bit processes for Enhanced Protected Mode*
☑ Enable DOM Storage
☐ Enable Enhanced Protected Mode*
☑ Enable Integrated Windows Authentication*
☑ Enable native XMLHTTP support
☑ Enable Windows Defender SmartScreen
☐ Send Do Not Track requests to sites you visit in Internet Explo
☐ Use SSL 3.0
☑ Use TLS 1.0
☑ Use TLS 1.1
☑ Use TLS 1.2
☑ Warn about certificate address mismatch*
☐ Warn if changing between secure and not secure mode
☑ Warn if POST submittal is redirected to a zone that does not p

*Takes effect after you restart your computer



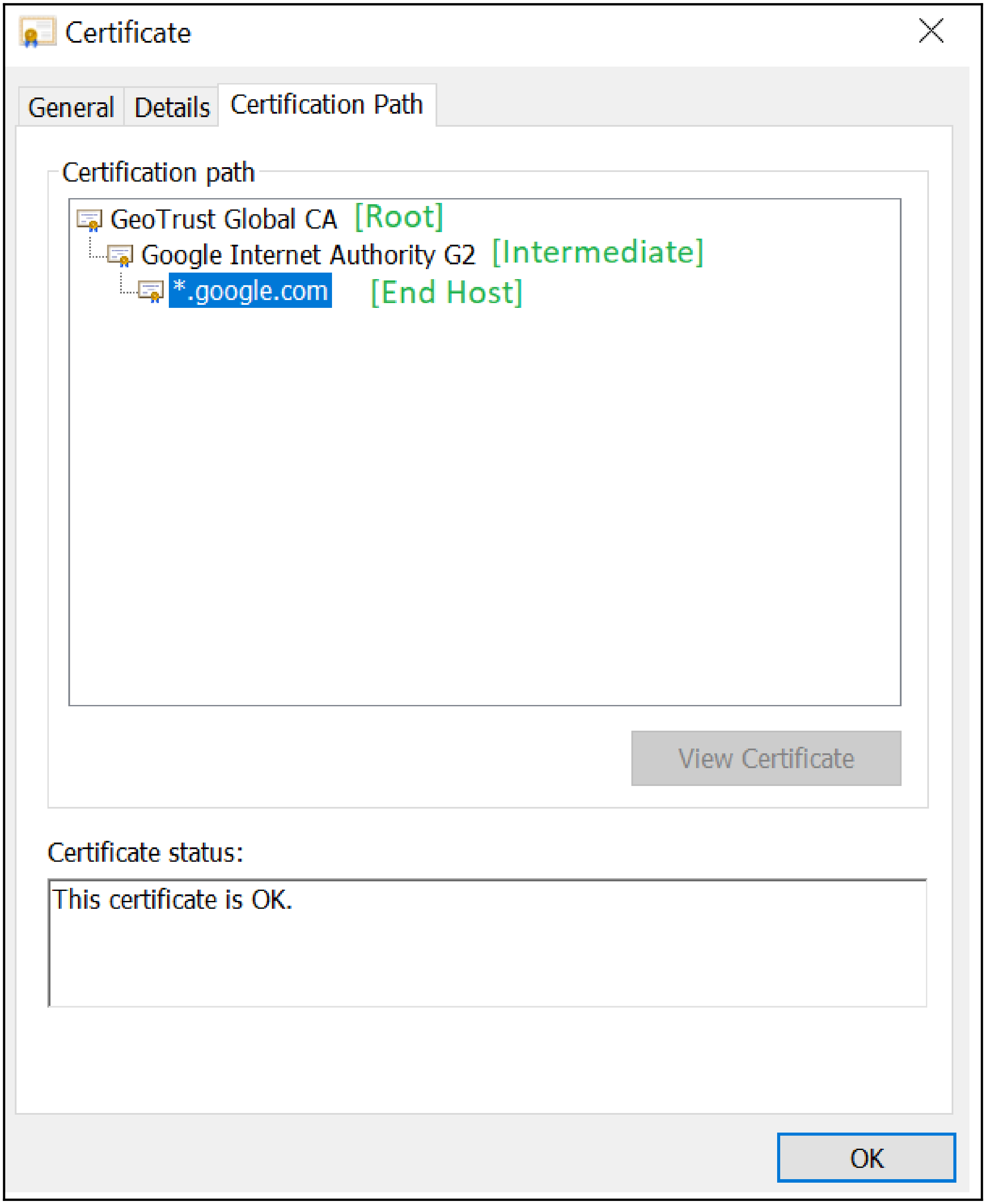
Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

Intended purpose: <All>

Issued To	Issued By	Expiration Date	Friendly N...
AddTrust External CA Root	AddTrust External C...	5/30/2020	The USER...
AffirmTrust Commercial	AffirmTrust Commer...	12/31/2030	AffirmTrus...
Baltimore CyberTrust Root	Baltimore CyberTrust...	5/13/2025	DigiCert B...
Certum CA	Certum CA	6/11/2027	Certum
Certum Trusted Network CA	Certum Trusted Net...	12/31/2029	Certum Tr...
Class 3 Public Primary Certif...	Class 3 Public Primar...	8/2/2028	VeriSign Cl...
COMODO RSA Certification ...	COMODO RSA Certif...	1/19/2038	COMODO ...
Copyright (c) 1997 Microsoft...	Copyright (c) 1997 ...	12/31/1999	Microsoft ...
D00155DD74F45	D00155DD74F45	1/2/3017	<None>



Certification path

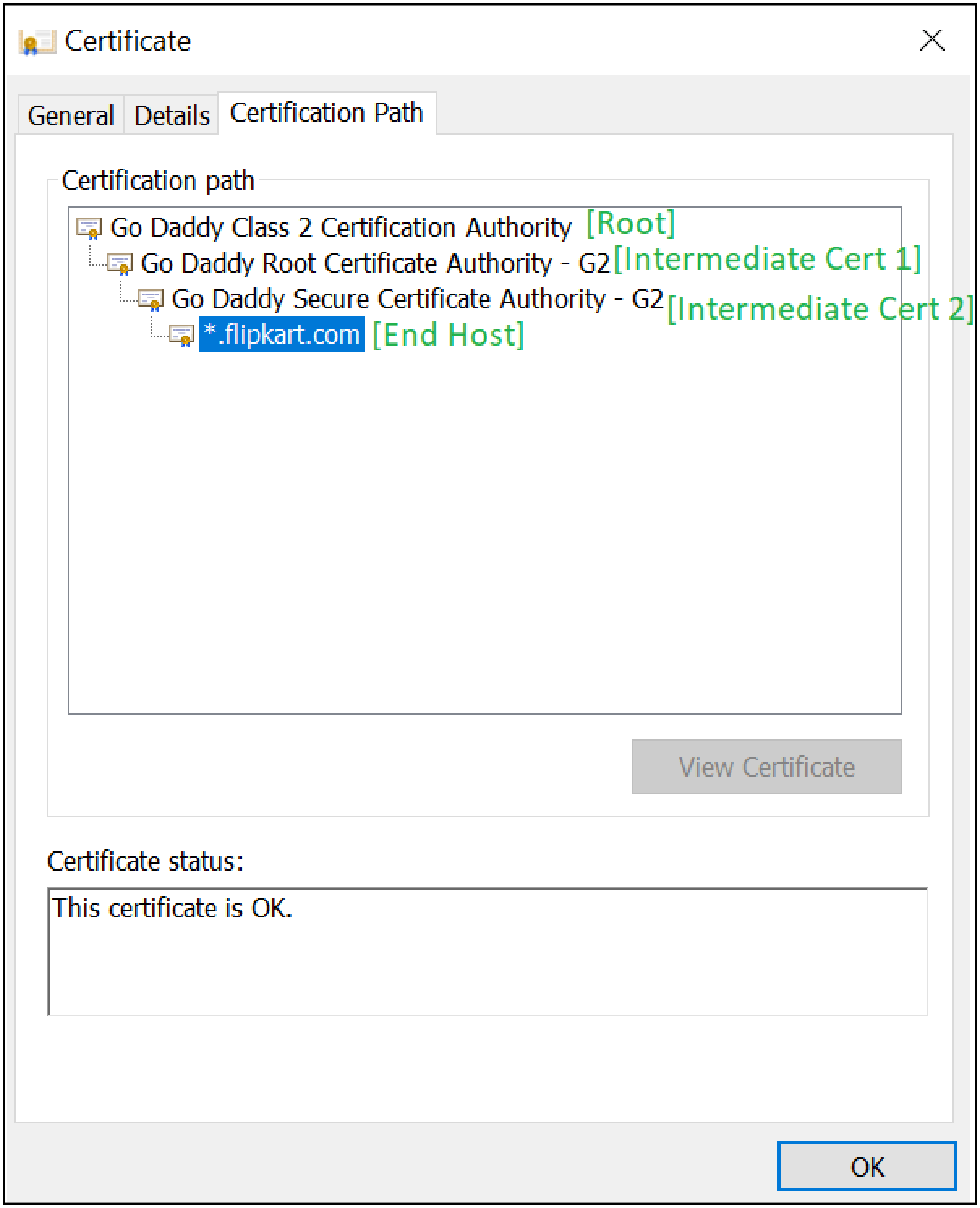
GeoTrust Global CA [Root]

Google Internet Authority G2 [Intermediate]

*.google.com [End Host]

Certificate status:

This certificate is OK.

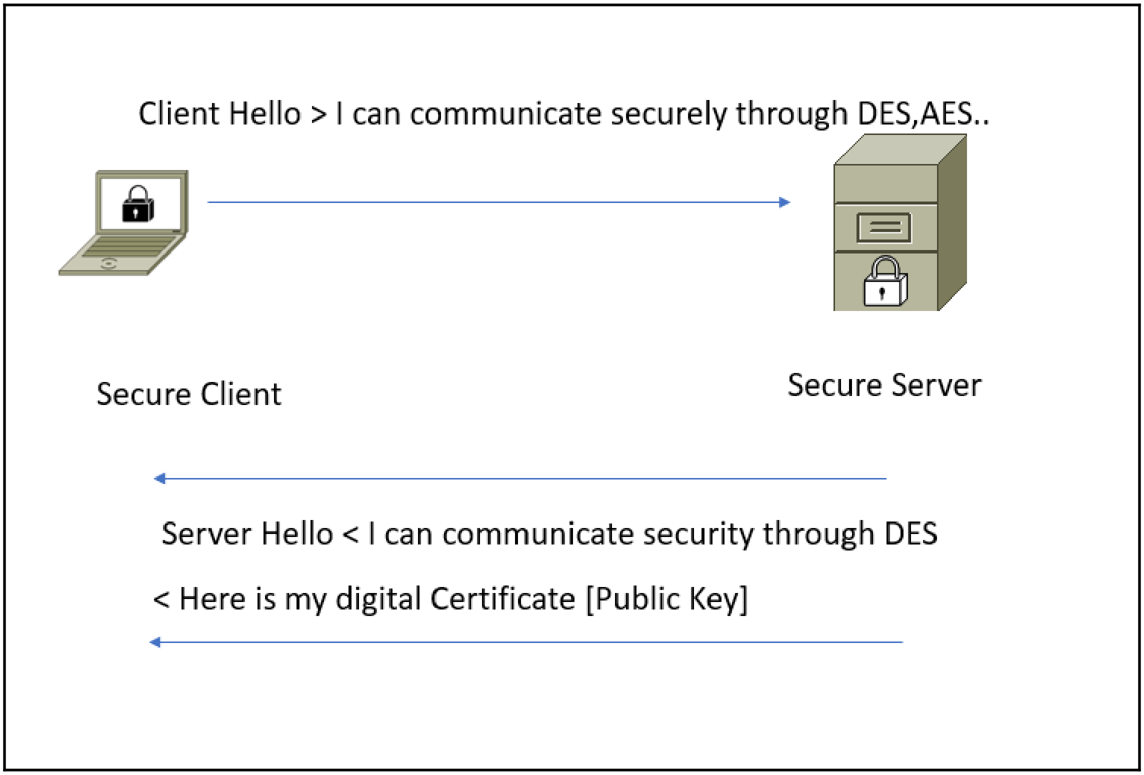


Certification path

Go Daddy Class 2 Certification Authority [Root]
Go Daddy Root Certificate Authority - G2[Intermediate Cert 1]
Go Daddy Secure Certificate Authority - G2[Intermediate Cert 2]
*.flipkart.com [End Host]

Certificate status:

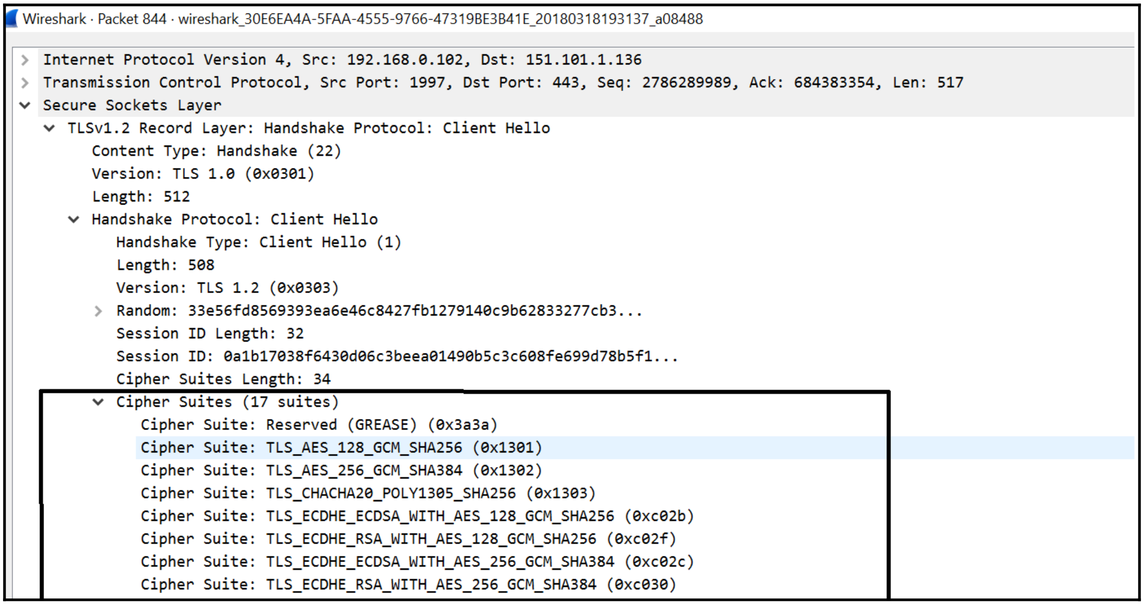
This certificate is OK.



Client Hello > I can communicate securely through DES,AES..

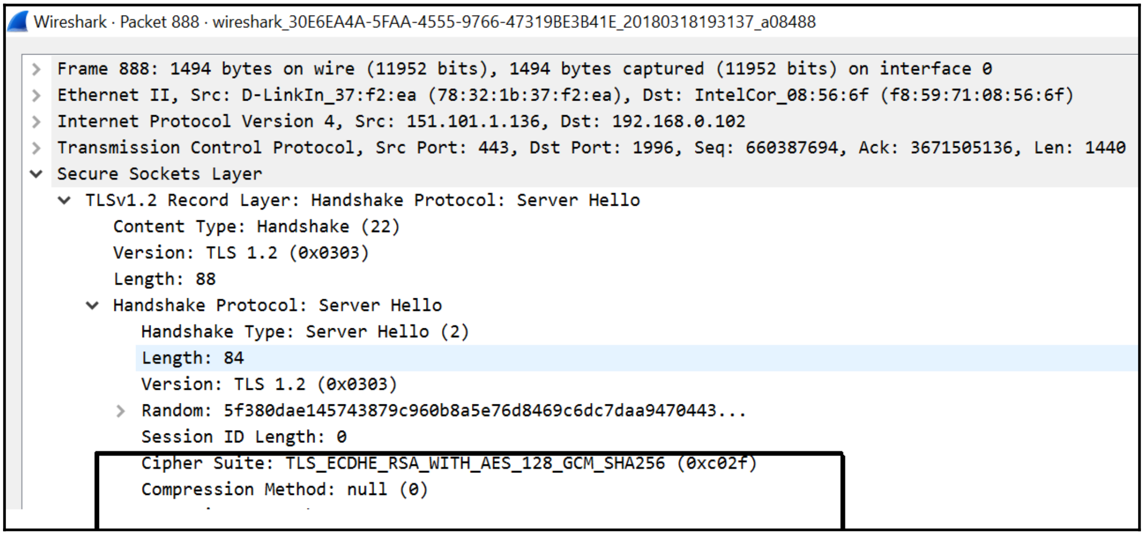
Server Hello < I can communicate security through DES

< Here is my digital Certificate [Public Key]



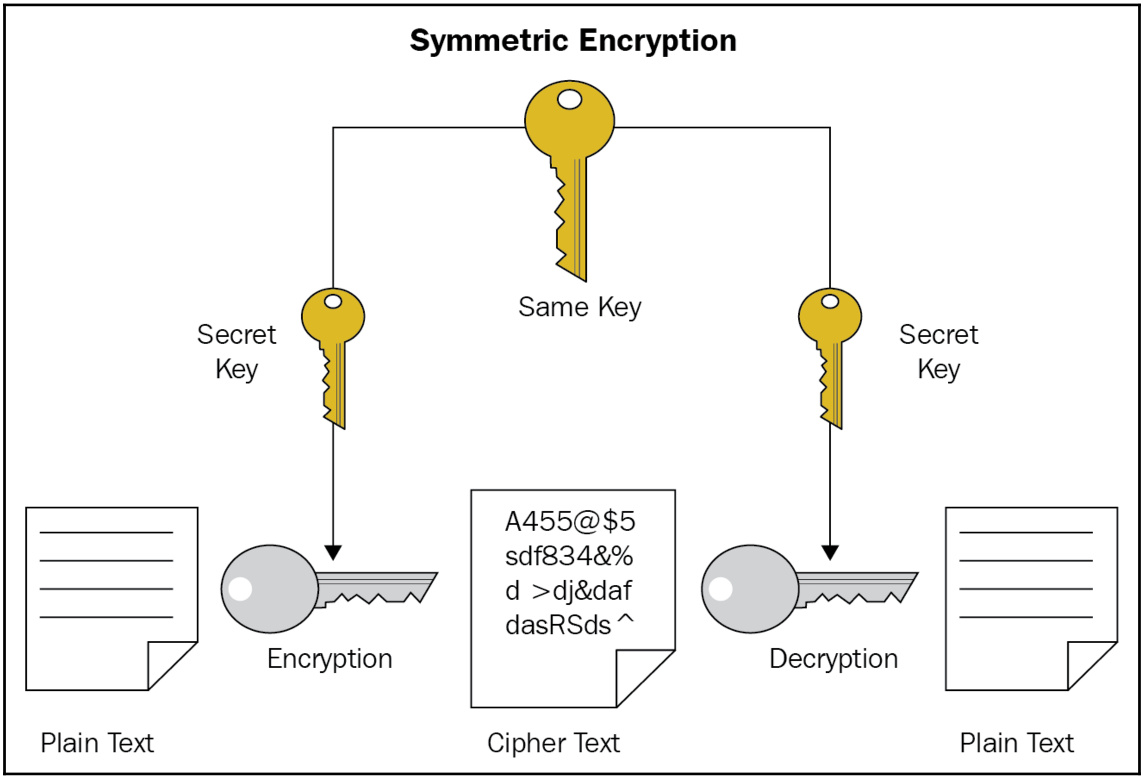
Wireshark · Packet 844 · wireshark_30E6EA4A-5FAA-4555-9766-47319BE3B41E_20180318193137_a08488

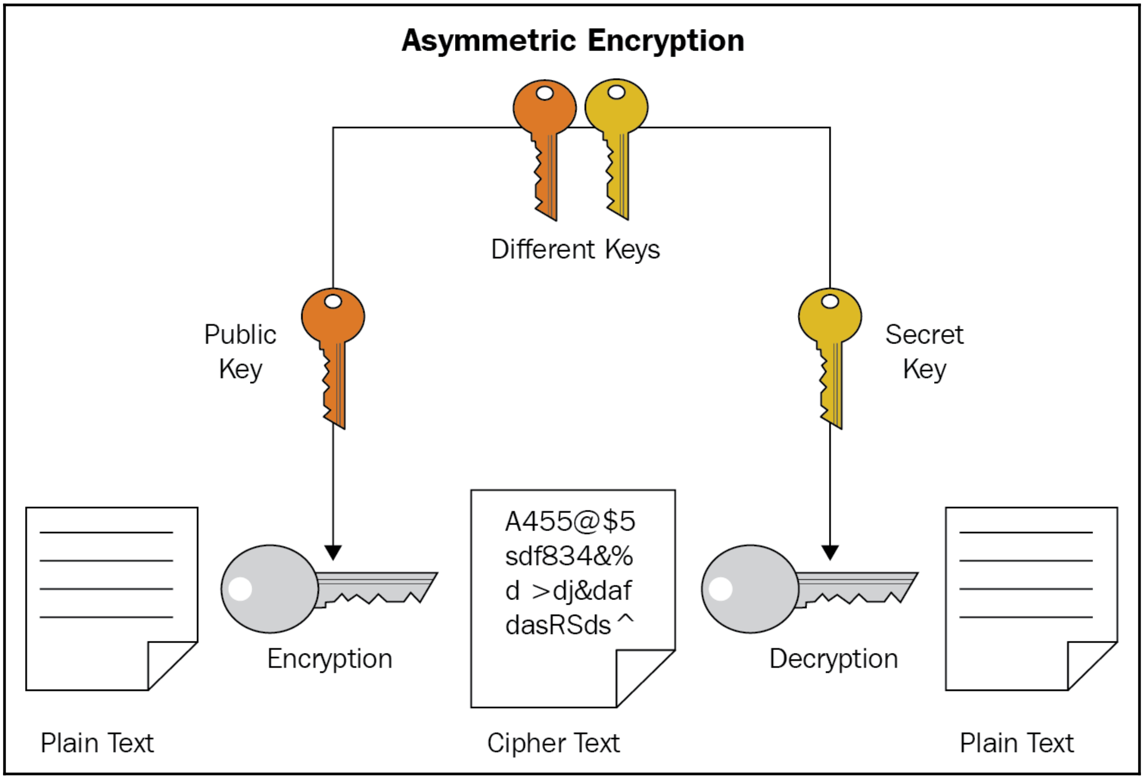
```
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 151.101.1.136
> Transmission Control Protocol, Src Port: 1997, Dst Port: 443, Seq: 2786289989, Ack: 684383354, Len: 517
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 512
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 508
        Version: TLS 1.2 (0x0303)
      > Random: 33e56fd8569393ea6e46c8427fb1279140c9b62833277cb3...
        Session ID Length: 32
        Session ID: 0a1b17038f6430d06c3beea01490b5c3c608fe699d78b5f1...
        Cipher Suites Length: 34
      v Cipher Suites (17 suites)
          Cipher Suite: Reserved (GREASE) (0x3a3a)
          Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
          Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
          Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
```

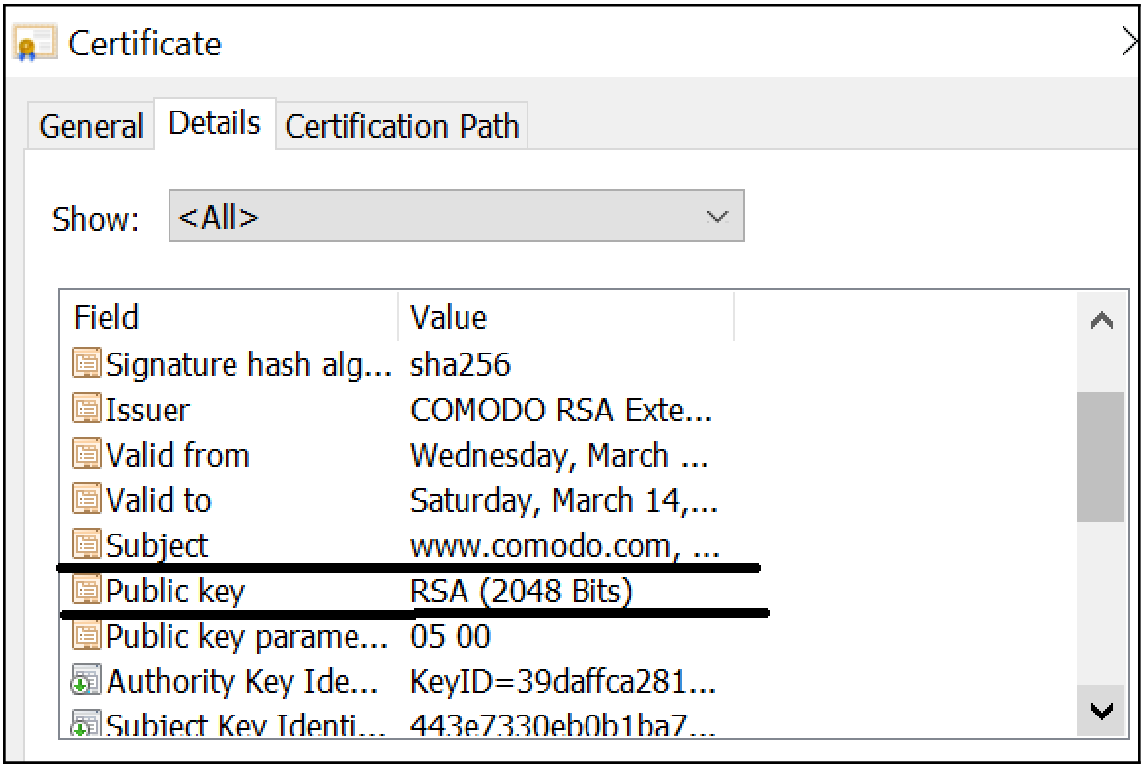


Wireshark · Packet 888 · wireshark_30E6EA4A-5FAA-4555-9766-47319BE3B41E_20180318193137_a08488

```
> Frame 888: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface 0
> Ethernet II, Src: D-LinkIn_37:f2:ea (78:32:1b:37:f2:ea), Dst: IntelCor_08:56:6f (f8:59:71:08:56:6f)
> Internet Protocol Version 4, Src: 151.101.1.136, Dst: 192.168.0.102
> Transmission Control Protocol, Src Port: 443, Dst Port: 1996, Seq: 660387694, Ack: 3671505136, Len: 1440
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 88
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 84
        Version: TLS 1.2 (0x0303)
      > Random: 5f380dae145743879c960b8a5e76d8469c6dc7daa9470443...
        Session ID Length: 0
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Compression Method: null (0)
```

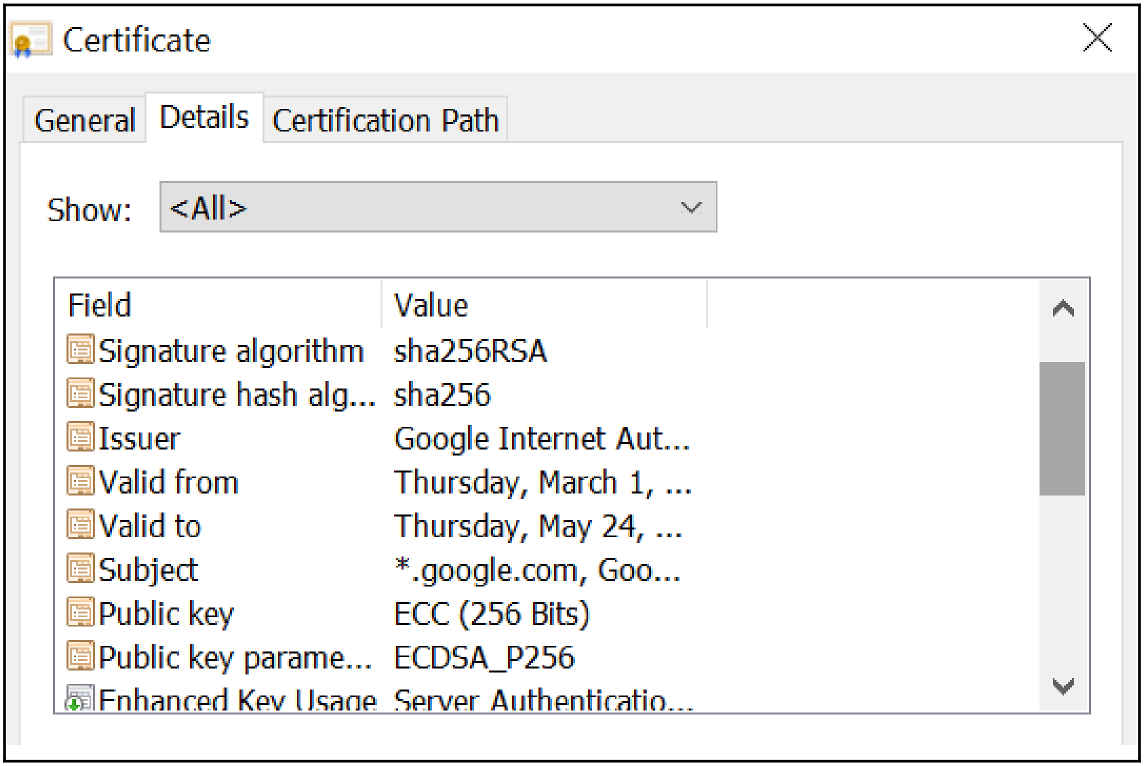

Symmetric Encryption
Same Key
Secret Key
Secret Key
A455@$5
sdf834&%
d >dj&daf
dasRSds ^
Encryption
Decryption
Plain Text
Cipher Text
Plain Text


Asymmetric Encryption
Different Keys
Public Key
Secret Key
A455@$5
sdf834&%
d >dj&daf
dasRSds ^
Encryption
Decryption
Plain Text
Cipher Text
Plain Text



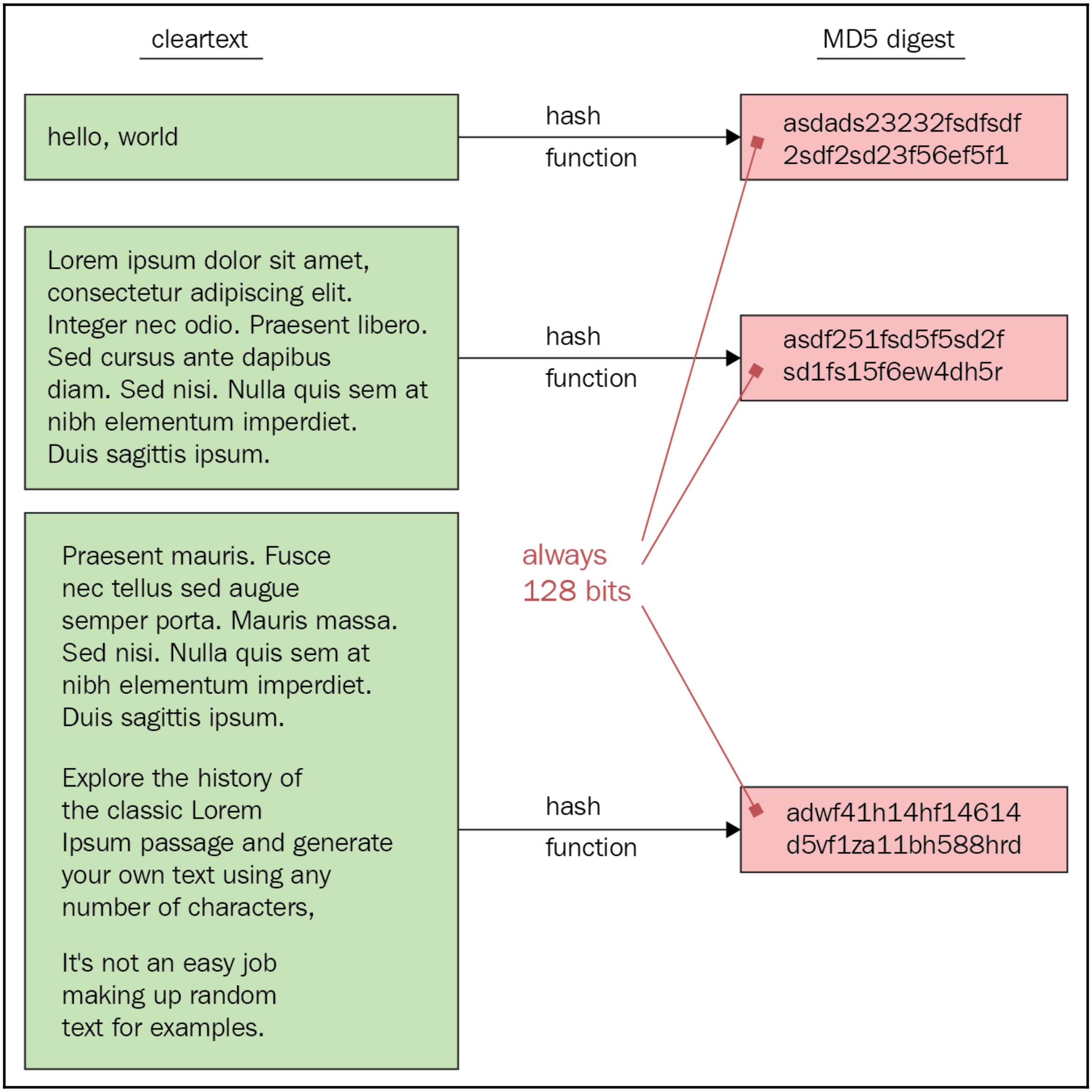
Show: <All>

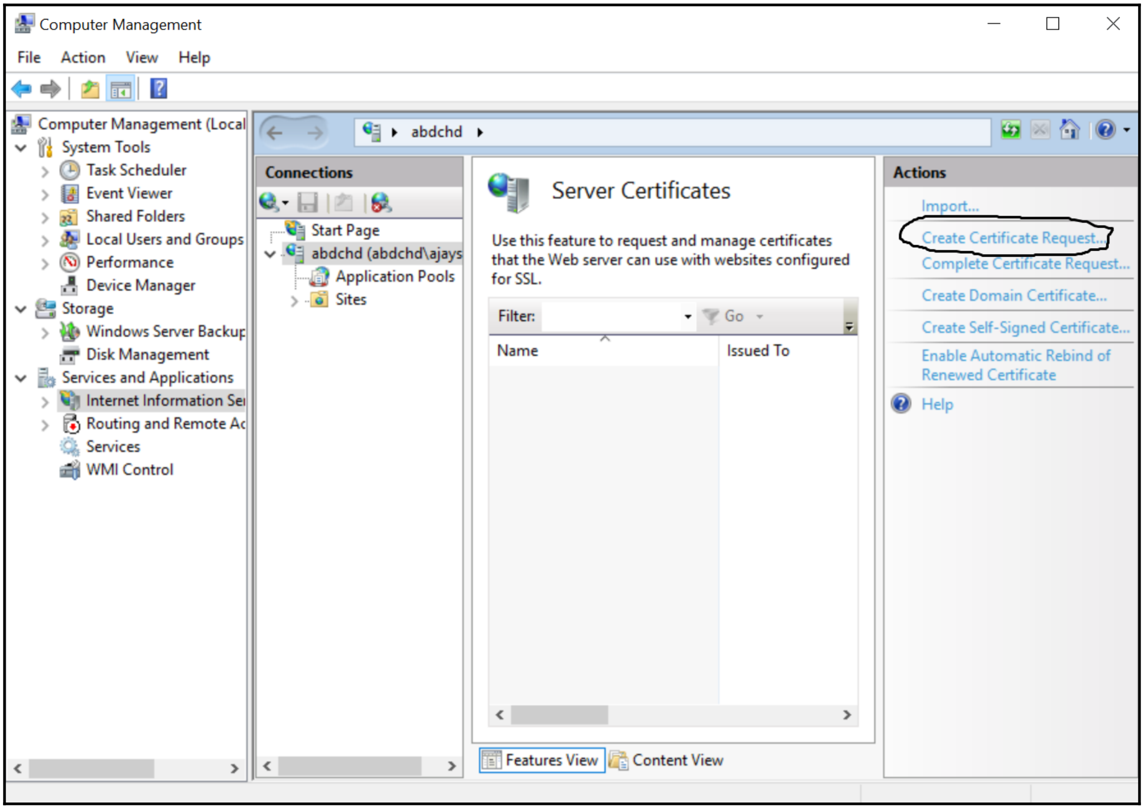
Field	Value
Signature hash alg...	sha256
Issuer	COMODO RSA Exte...
Valid from	Wednesday, March ...
Valid to	Saturday, March 14,...
Subject	www.comodo.com, ...
Public key	RSA (2048 Bits)
Public key parame...	05 00
Authority Key Ide...	KeyID=39daffca281...
Subject Key Identi...	443e7330eb0b1ba7...



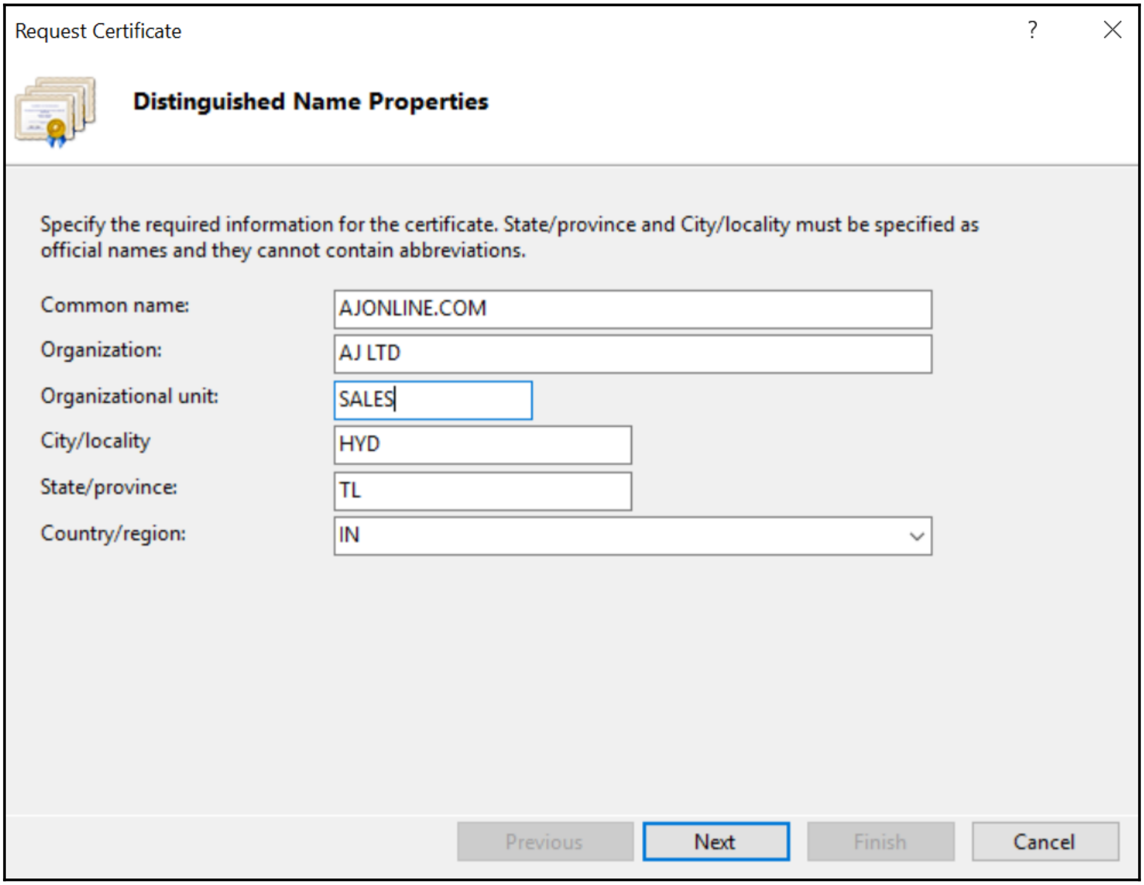
Show: <All>

Field	Value
Signature algorithm	sha256RSA
Signature hash alg...	sha256
Issuer	Google Internet Aut...
Valid from	Thursday, March 1, ...
Valid to	Thursday, May 24, ...
Subject	*.google.com, Goo...
Public key	ECC (256 Bits)
Public key parame...	ECDSA_P256
Enhanced Key Usage	Server Authenticatio...


cleartext
MD5 digest
hello, world
hash
function
asdads23232fsdfsdf
2sdf2sd23f56ef5f1
Lorem ipsum dolor sit amet,
consectetur adipiscing elit.
Integer nec odio. Praesent libero.
Sed cursus ante dapibus
diam. Sed nisi. Nulla quis sem at
nibh elementum imperdiet.
Duis sagittis ipsum.
hash
function
asdf251fsd5f5sd2f
sd1fs15f6ew4dh5r
Praesent mauris. Fusce
nec tellus sed augue
semper porta. Mauris massa.
Sed nisi. Nulla quis sem at
nibh elementum imperdiet.
Duis sagittis ipsum.
Explore the history of
the classic Lorem
Ipsum passage and generate
your own text using any
number of characters,
It's not an easy job
making up random
text for examples.
always
128 bits
hash
function
adwf41h14hf14614
d5vf1za11bh588hrd

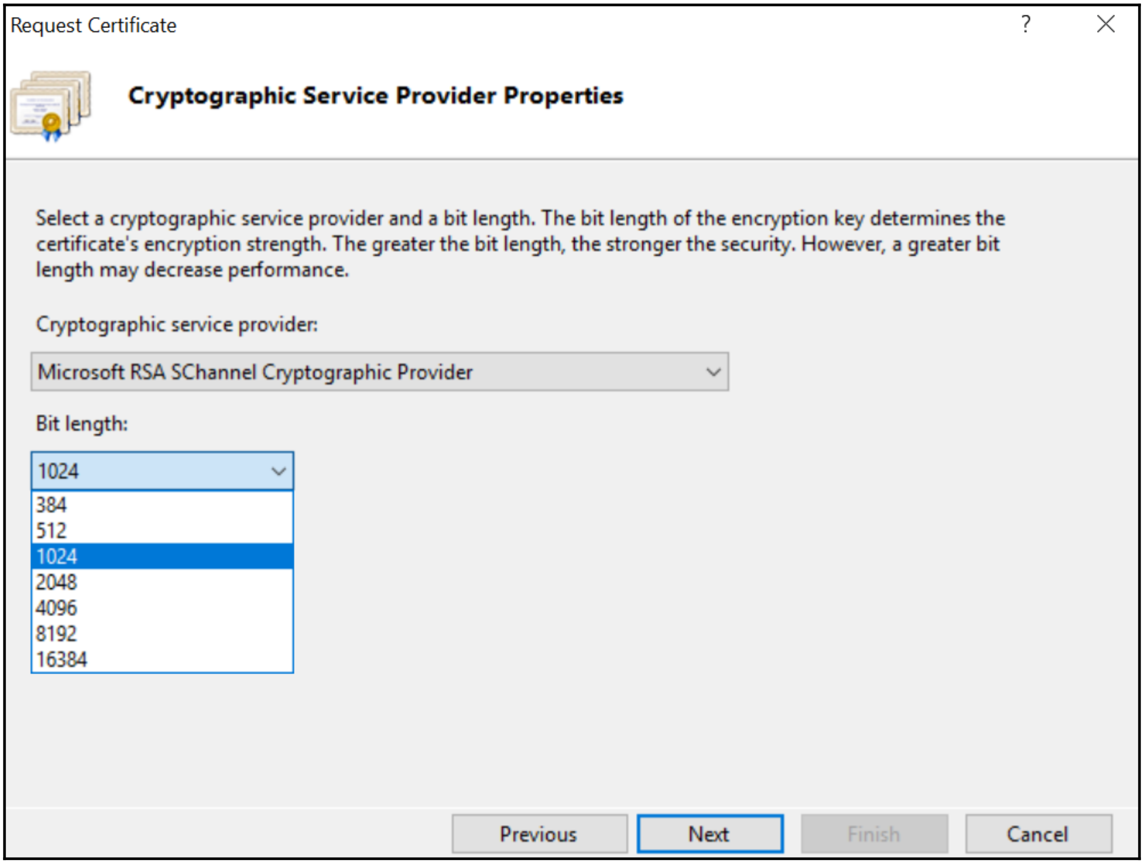


Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.



Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	AJONLINE.COM
Organization:	AJ LTD
Organizational unit:	SALES
City/locality	HYD
State/province:	TL
Country/region:	IN



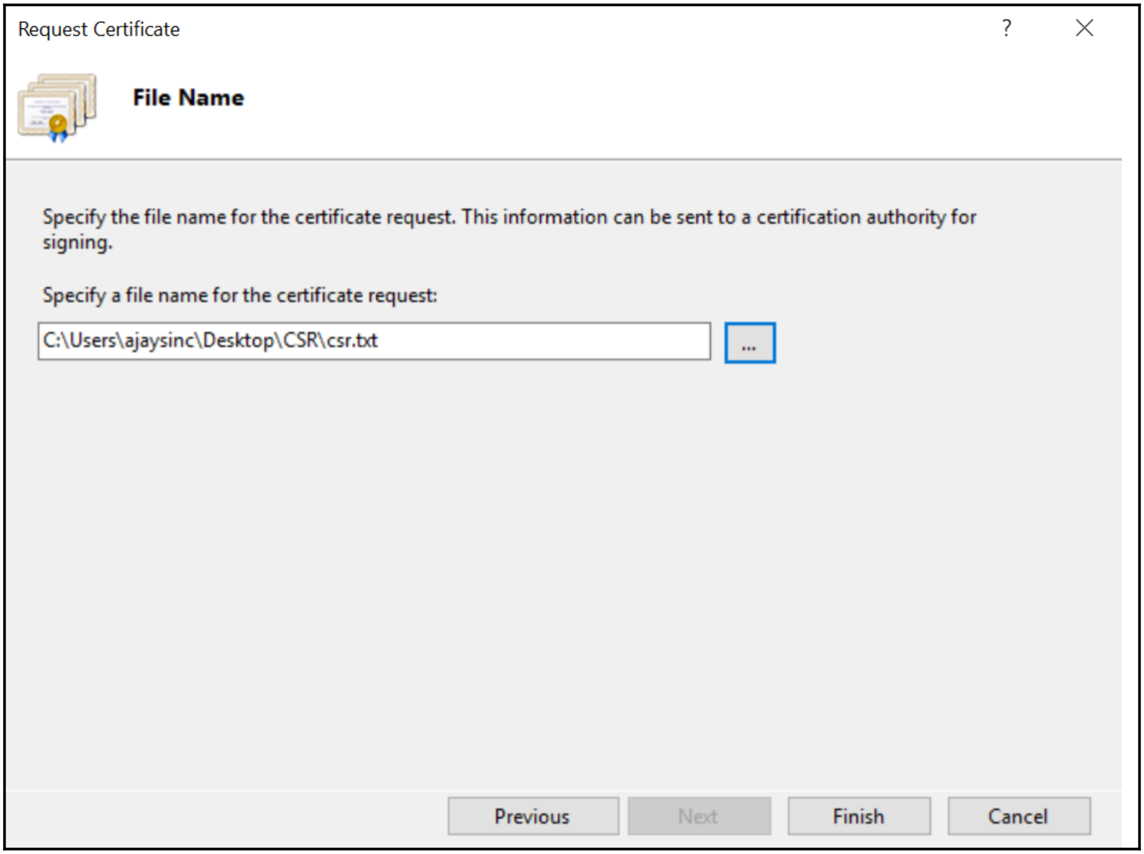
Request Certificate

Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider

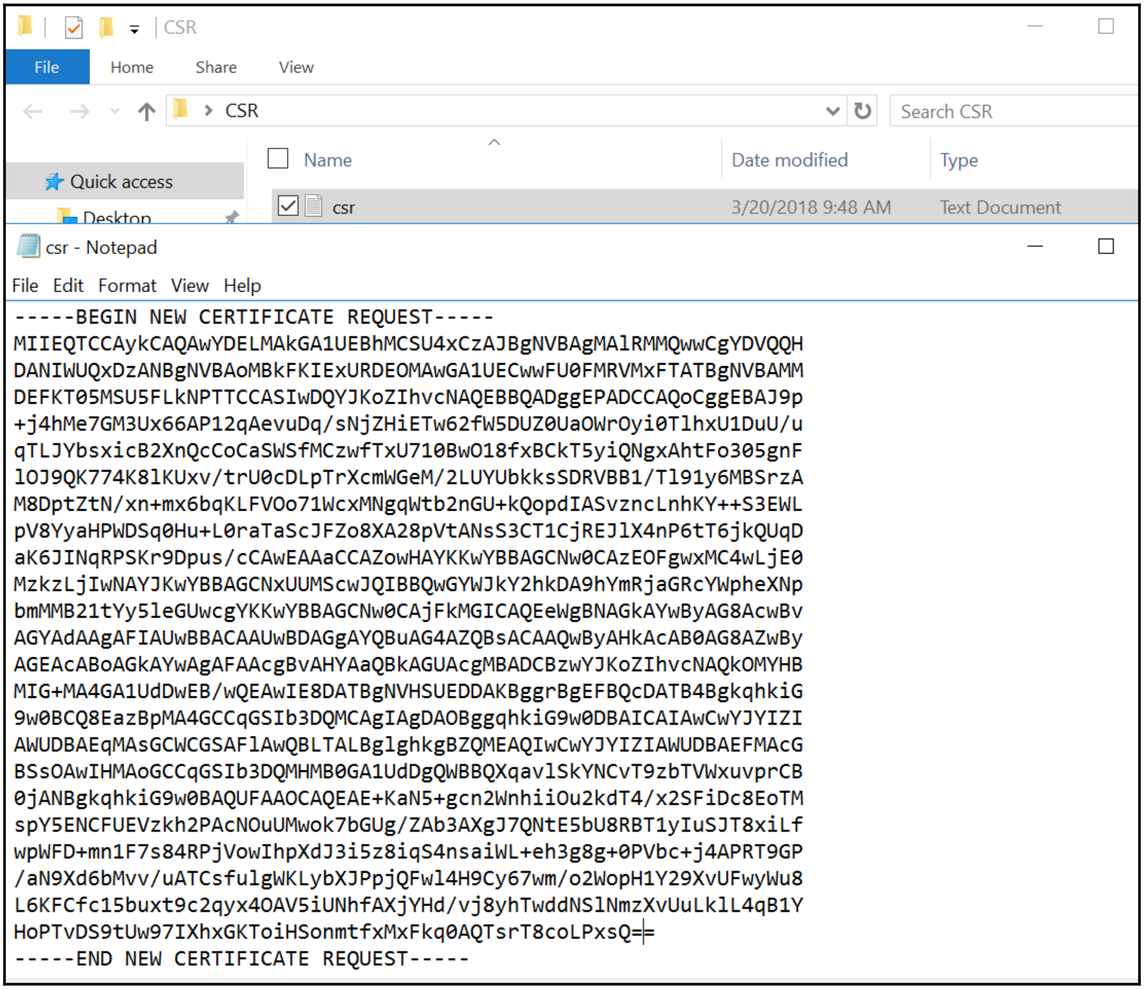
Bit length: 1024



Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

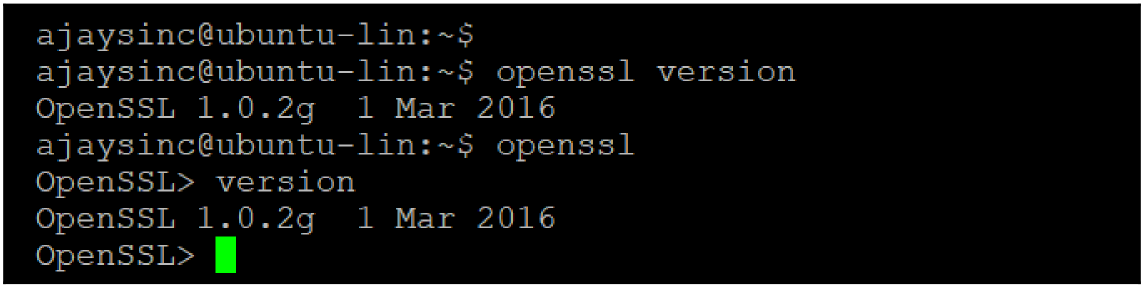
Specify a file name for the certificate request:

C:\Users\ajaysinc\Desktop\CSR\csr.txt

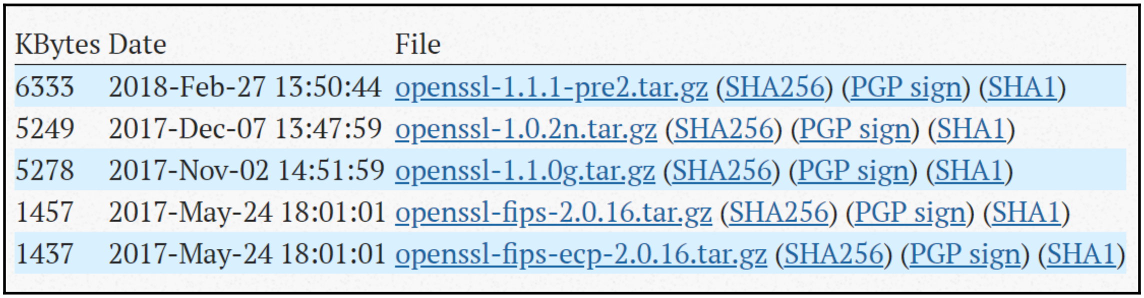


Name	Date modified	Type
☑ csr	3/20/2018 9:48 AM	Text Document

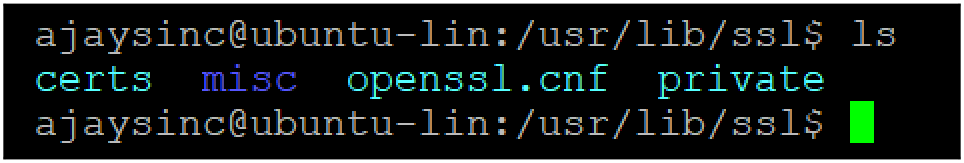
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEQTCCAykCAQAwYDELMAkGA1UEBhMCSU4xCzAJBgNVBAgMAlRMMQwwCgYDVQQH
DANIWUQxDzANBgNVBAoMBkFKIExURDEOMAwGA1UECwwFU0FMRVMxFTATBgNVBAMM
DEFKT05MSU5FLkNPTTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ9p
+j4hMe7GM3Ux66AP12qAevuDq/sNjZHiETw62fW5DUZ0UaOWrOyi0TlhxU1DuU/u
qTLJYbsxicB2XnQcCoCaSWSfMCzwfTxU710BwO18fxBCkT5yiQNgxAhtFo305gnF
lOJ9QK774K8lKUxv/trU0cDLpTrXcmWGeM/2LUYUbkksSDRVBB1/Tl91y6MBSrzA
M8DptZtN/xn+mx6bqKLFVOo71WcxMNgqWtb2nGU+kQopdIASvzncLnhKY++S3EWL
pV8YyaHPWDSq0Hu+L0raTaScJFZo8XA28pVtANsS3CT1CjREJlX4nP6tT6jkQUqD
aK6JINqRPSKr9Dpus/cCAwEAAaCCAZowHAYKKwYBBAGCNw0CAzEOFgwxMC4wLjE0
MzkzLjIwNAYJKwYBBAGCNxUUMScwJQIBBQwGYWJkY2hkDA9hYmRjaGRcYWpheXNp
bmMMB21tYy5leGUwcgYKKwYBBAGCNw0CAjFkMGICAQEeWgBNAGkAYwByAG8AcwBv
AGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuAG4AZQBsACAAQwByAHkAcAB0AG8AZwBy
AGEAcABoAGkAYwAgAFAAcgBvAHYAaQBkAGUAcgMBADCBzwYJKoZIhvcNAQkOMYHB
MIG+MA4GA1UdDwEB/wQEAwIE8DATBgNVHSUEDDAKBggrBgEFBQcDATB4BgkqhkiG
9w0BCQ8EazBpMA4GCCqGSIb3DQMCAgIAgDAOBggqhkiG9w0DBAICAIAwCwYJYIZI
AWUDBAEqMAsGCWCGSAFlAwQBLTALBglghkgBZQMEAQIwCwYJYIZIAWUDBAEFMAcG
BSsOAwIHMAoGCCqGSIb3DQMHMB0GA1UdDgQWBBQXqavlSkYNCvT9zbTVWxuvprCB
0jANBgkqhkiG9w0BAQUFAAOCAQEAE+KaN5+gcn2WnhiiOu2kdT4/x2SFiDc8EoTM
spY5ENCFUEVzkh2PAcNOuUMwok7bGUg/ZAb3AXgJ7QNtE5bU8RBT1yIuSJT8xiLf
wpWFD+mn1F7s84RPjVowIhpXdJ3i5z8iqS4nsaiWL+eh3g8g+0PVbc+j4APRT9GP
/aN9Xd6bMvv/uATCsfulgWKLybXJPpjQFwl4H9Cy67wm/o2WopH1Y29XvUFwyWu8
L6KFCfc15buxt9c2qyx4OAV5iUNhfAXjYHd/vj8yhTwddNSlNmzXvUuLklL4qB1Y
HoPTvDS9tUw97IXhxGKToiHSonmtfxMxFkq0AQTsrT8coLPxsQ==
-----END NEW CERTIFICATE REQUEST-----
```



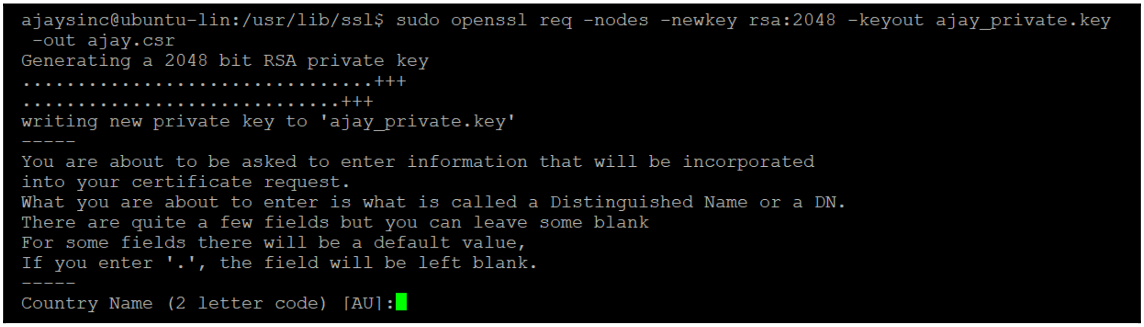
```
ajaysinc@ubuntu-lin:~$
ajaysinc@ubuntu-lin:~$ openssl version
OpenSSL 1.0.2g  1 Mar 2016
ajaysinc@ubuntu-lin:~$ openssl
OpenSSL> version
OpenSSL 1.0.2g  1 Mar 2016
OpenSSL>
```



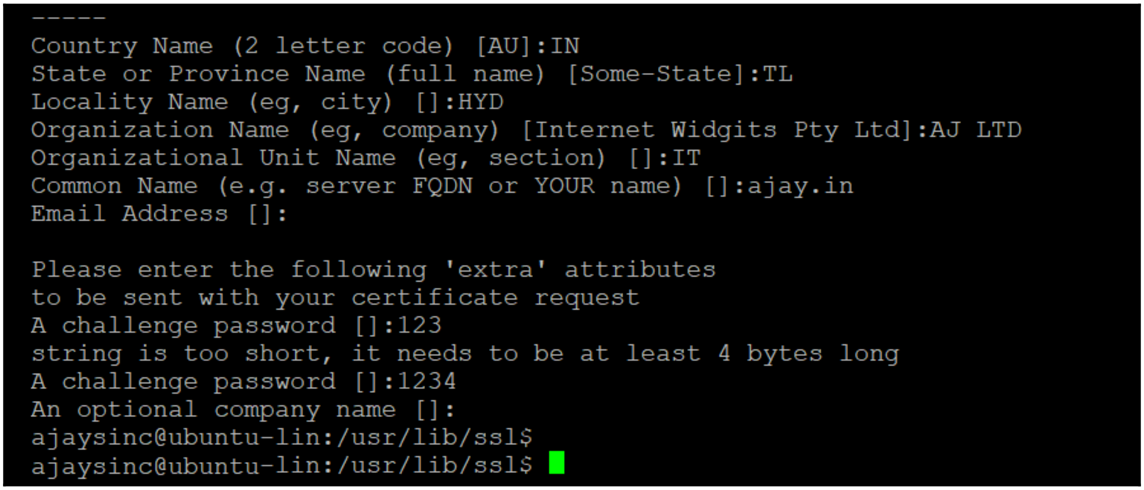
KBytes	Date	File
6333	2018-Feb-27 13:50:44	openssl-1.1.1-pre2.tar.gz (SHA256) (PGP sign) (SHA1)
5249	2017-Dec-07 13:47:59	openssl-1.0.2n.tar.gz (SHA256) (PGP sign) (SHA1)
5278	2017-Nov-02 14:51:59	openssl-1.1.0g.tar.gz (SHA256) (PGP sign) (SHA1)
1457	2017-May-24 18:01:01	openssl-fips-2.0.16.tar.gz (SHA256) (PGP sign) (SHA1)
1437	2017-May-24 18:01:01	openssl-fips-ecp-2.0.16.tar.gz (SHA256) (PGP sign) (SHA1)



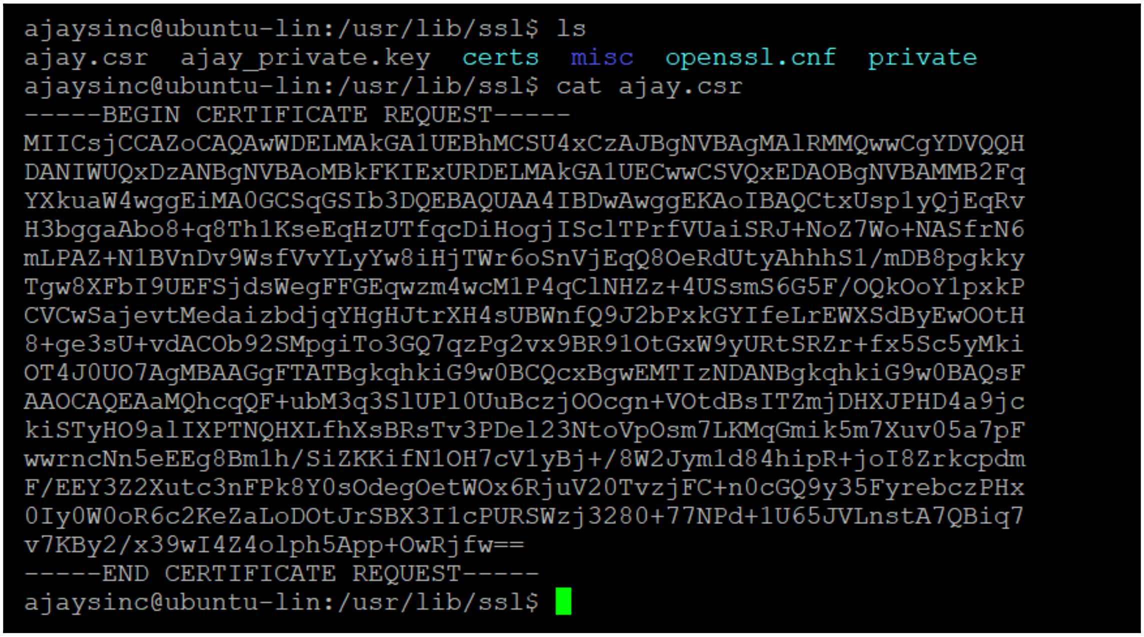
```
ajaysinc@ubuntu-lin:/usr/lib/ssl$ ls
certs  misc  openssl.cnf  private
ajaysinc@ubuntu-lin:/usr/lib/ssl$
```



```
ajaysinc@ubuntu-lin:/usr/lib/ssl$ sudo openssl req -nodes -newkey rsa:2048 -keyout ajay_private.key
 -out ajay.csr
Generating a 2048 bit RSA private key
................................+++
.............................+++
writing new private key to 'ajay_private.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
```

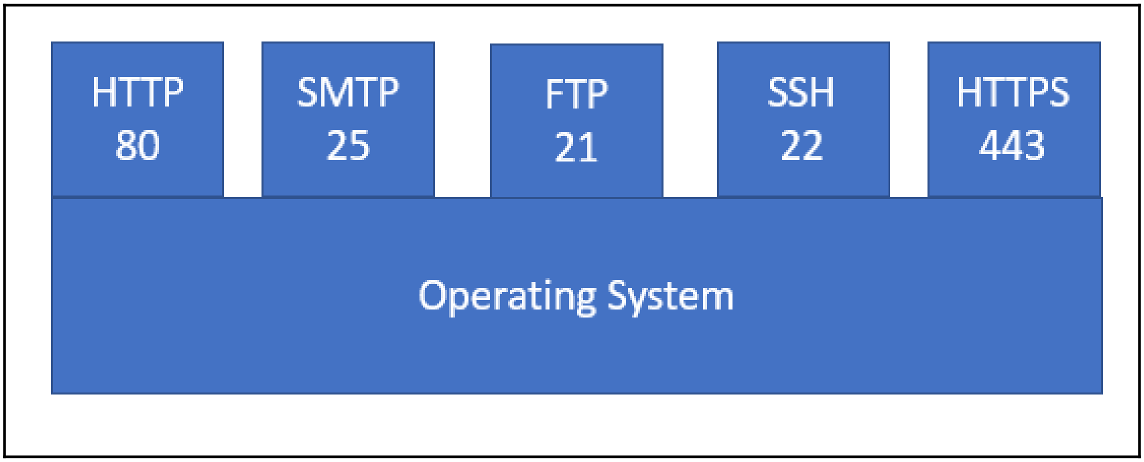


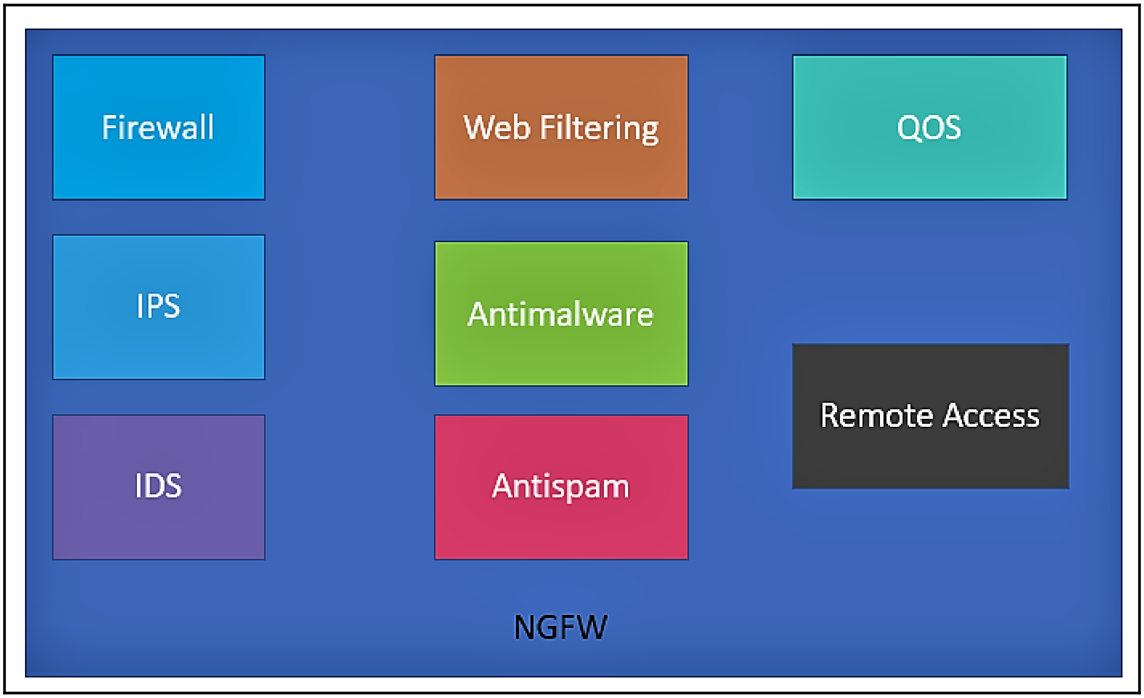
```
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:TL
Locality Name (eg, city) []:HYD
Organization Name (eg, company) [Internet Widgits Pty Ltd]:AJ LTD
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:ajay.in
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123
string is too short, it needs to be at least 4 bytes long
A challenge password []:1234
An optional company name []:
ajaysinc@ubuntu-lin:/usr/lib/ssl$
ajaysinc@ubuntu-lin:/usr/lib/ssl$
```

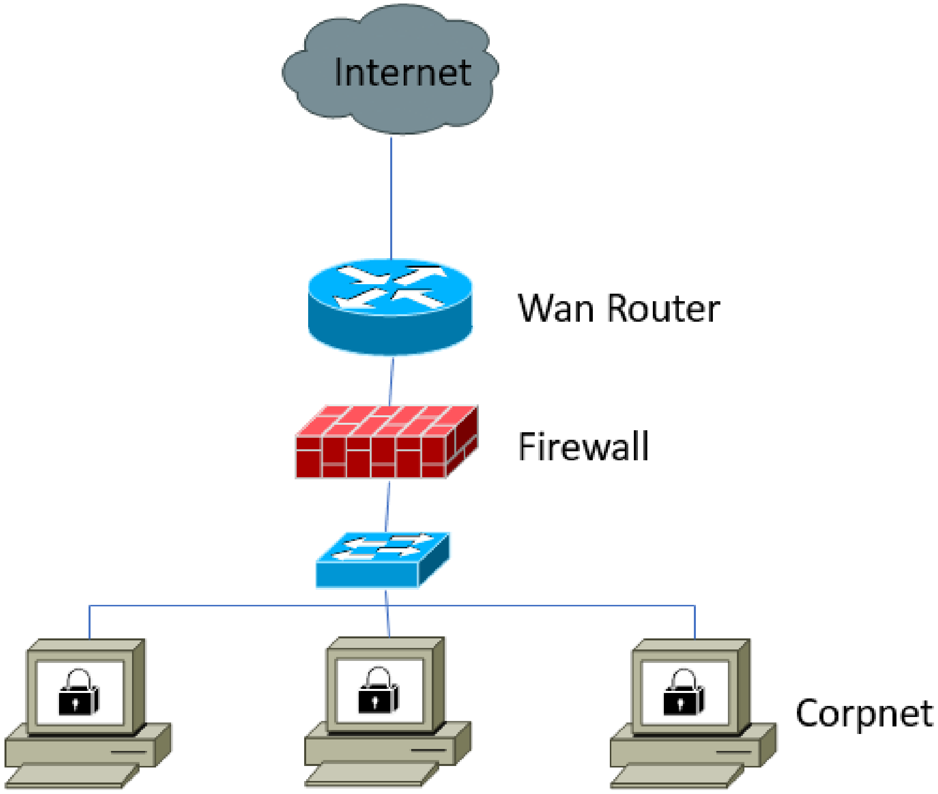


```
ajaysinc@ubuntu-lin:/usr/lib/ssl$ ls
ajay.csr  ajay_private.key  certs  misc  openssl.cnf  private
ajaysinc@ubuntu-lin:/usr/lib/ssl$ cat ajay.csr
-----BEGIN CERTIFICATE REQUEST-----
MIICsjCCAZoCAQAwWDELMAkGA1UEBhMCSU4xCzAJBgNVBAgMAlRMMQwwCgYDVQQH
DANIWUQxDzANBgNVBAoMBkFKIExURDELMAkGA1UECwwCSVQxEDAOBgNVBAMMB2Fq
YXkuaW4wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCtxUsp1yQjEqRv
H3bggaAbo8+q8Th1KseEqHzUTfqcDiHogjISclTPrfVUaiSRJ+NoZ7Wo+NASfrN6
mLPAZ+N1BVnDv9WsfVvYLyYw8iHjTWr6oSnVjEqQ8OeRdUtyAhhhS1/mDB8pgkky
Tgw8XFbI9UEFSjdsWegFFGEqwzm4wcM1P4qClNHZz+4USsmS6G5F/OQkOoY1pxkP
CVCwSajevtMedaizbdjqYHgHJtrXH4sUBWnfQ9J2bPxkGYIfeLrEWXSdByEwOOtH
8+ge3sU+vdACOb92SMpgiTo3GQ7qzPg2vx9BR91OtGxW9yURtSRZr+fx5Sc5yMki
OT4J0UO7AgMBAAGgFTATBgkqhkiG9w0BCQcxBgwEMTIzNDANBgkqhkiG9w0BAQsF
AAOCAQEAaMQhcqQF+ubM3q3SlUPl0UuBczjOOcgn+VOtdBsITZmjDHXJPHD4a9jc
kiSTyHO9alIXPTNQHXLfhXsBRsTv3PDel23NtoVpOsm7LKMqGmik5m7Xuv05a7pF
wwrncNn5eEEg8Bm1h/SiZKKifN1OH7cV1yBj+/8W2Jym1d84hipR+joI8Zrkcpdm
F/EEY3Z2Xutc3nFPk8Y0sOdegOetWOx6RjuV20TvzjFC+n0cGQ9y35FyrebczPHx
0Iy0W0oR6c2KeZaLoDOtJrSBX3I1cPURSWzj3280+77NPd+1U65JVLnstA7QBiq7
v7KBy2/x39wI4Z4olph5App+OwRjfw==
-----END CERTIFICATE REQUEST-----
ajaysinc@ubuntu-lin:/usr/lib/ssl$
```

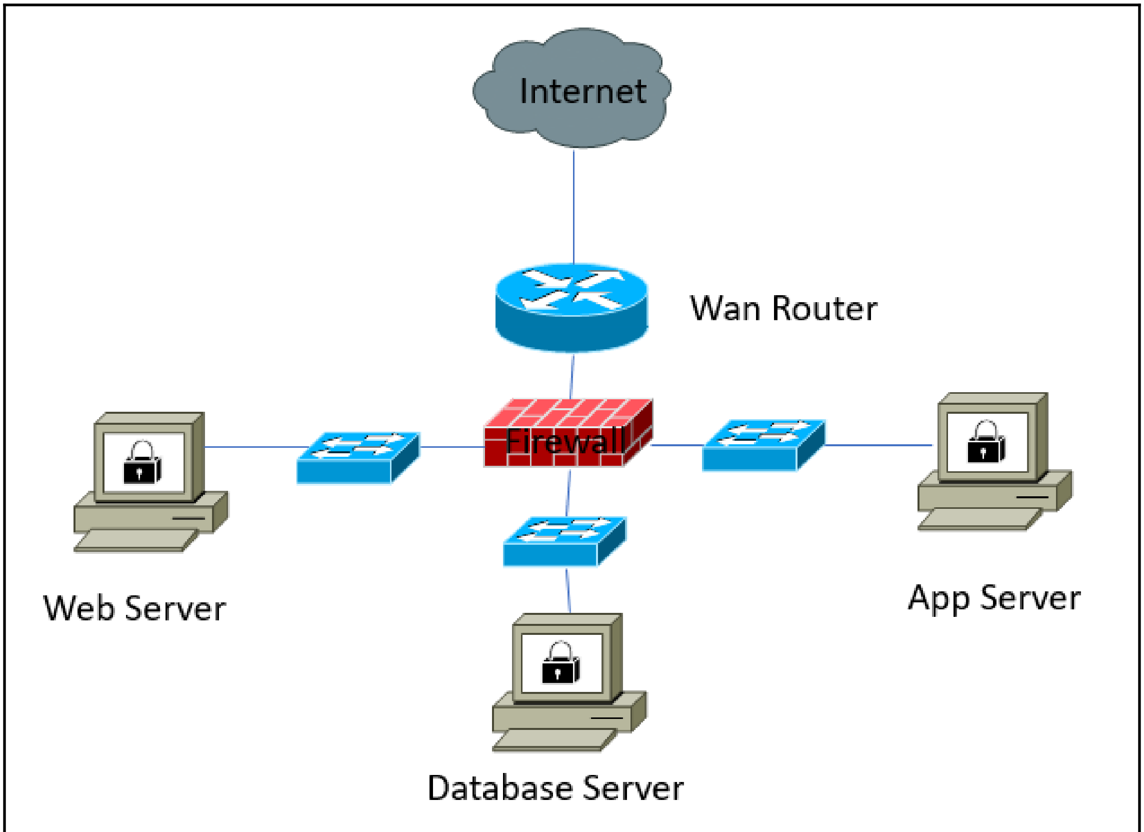
Chapter 10: Firewall detection



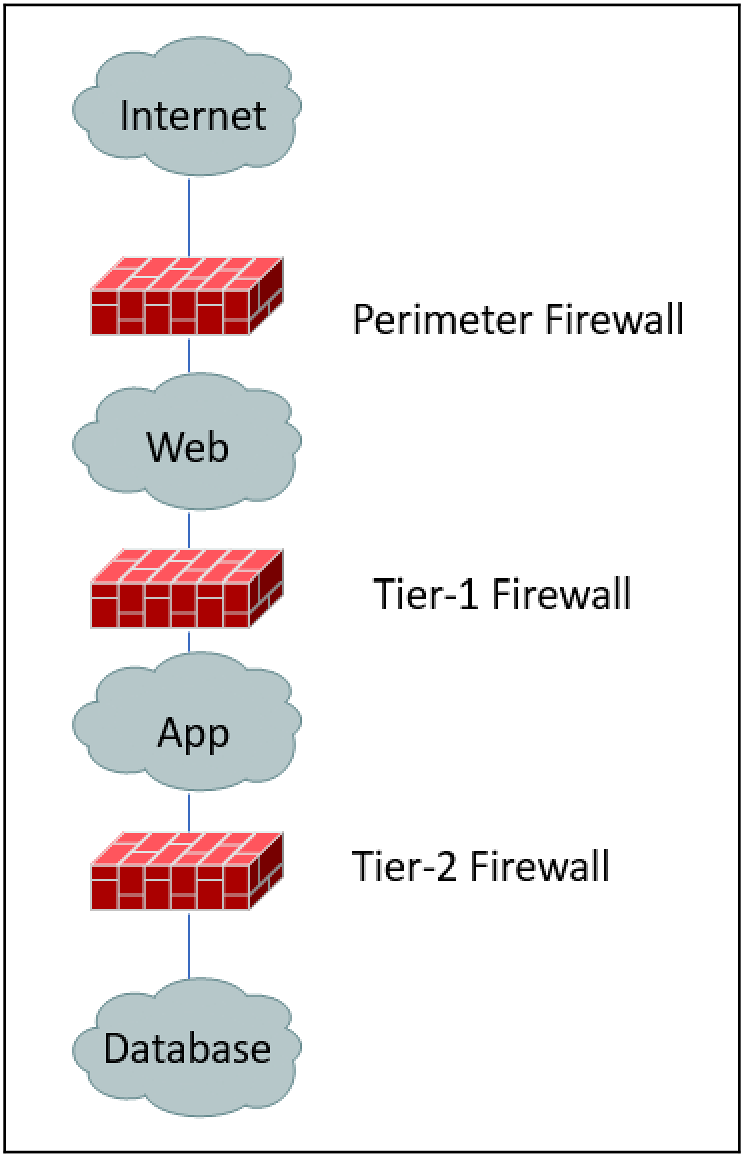


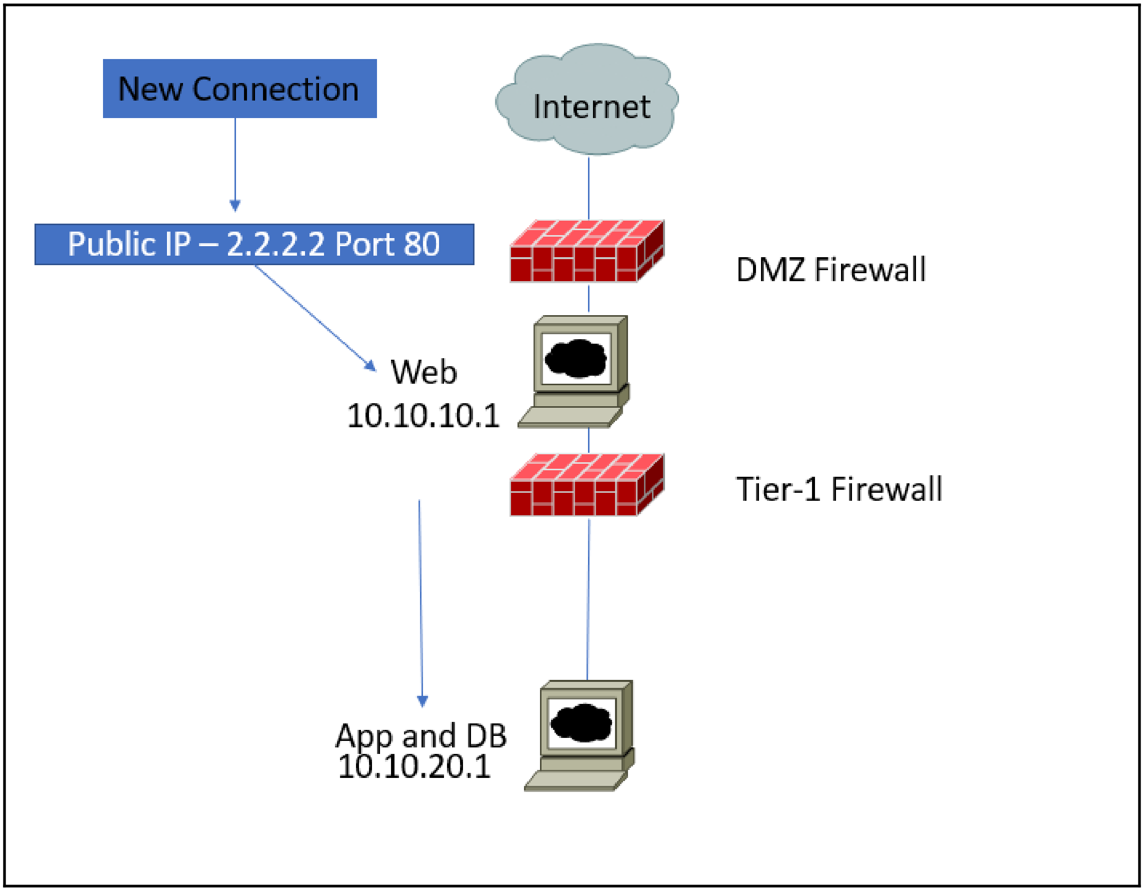


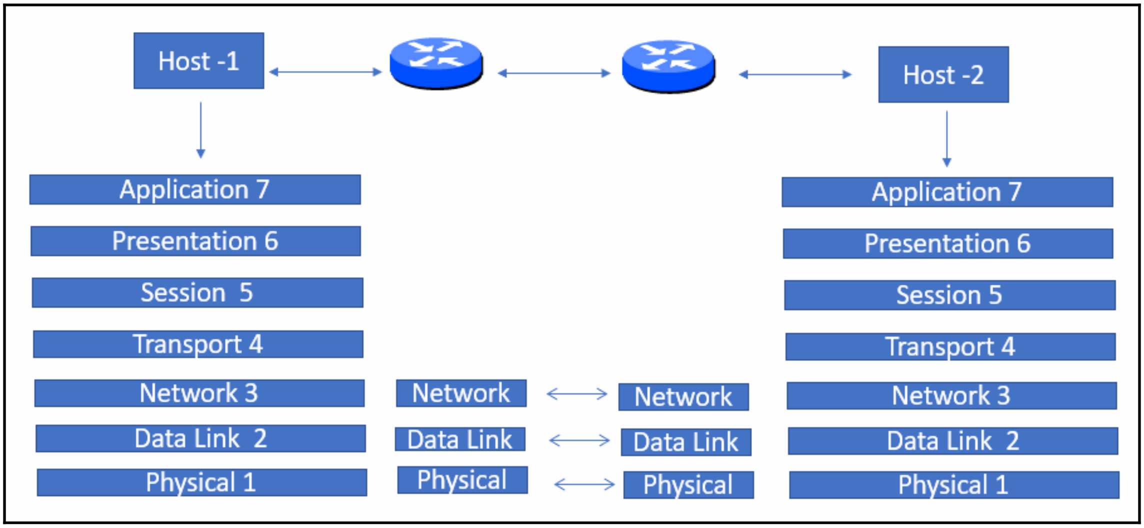
Single Firewall Architecture

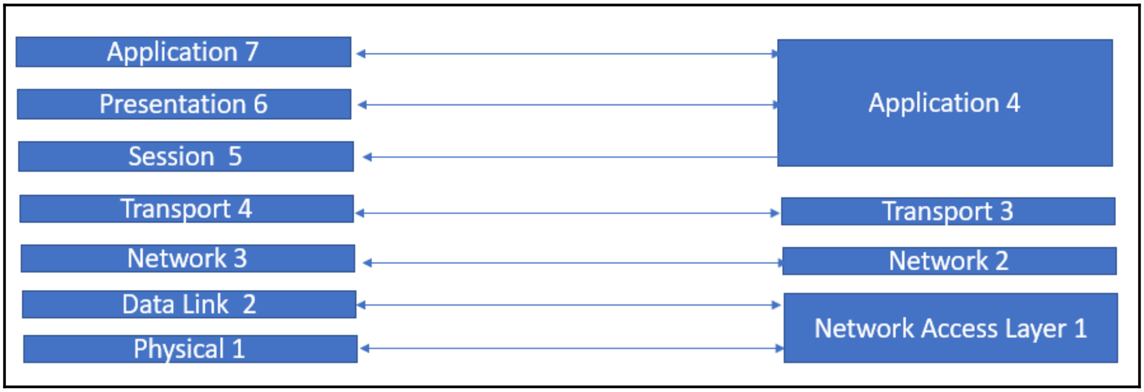


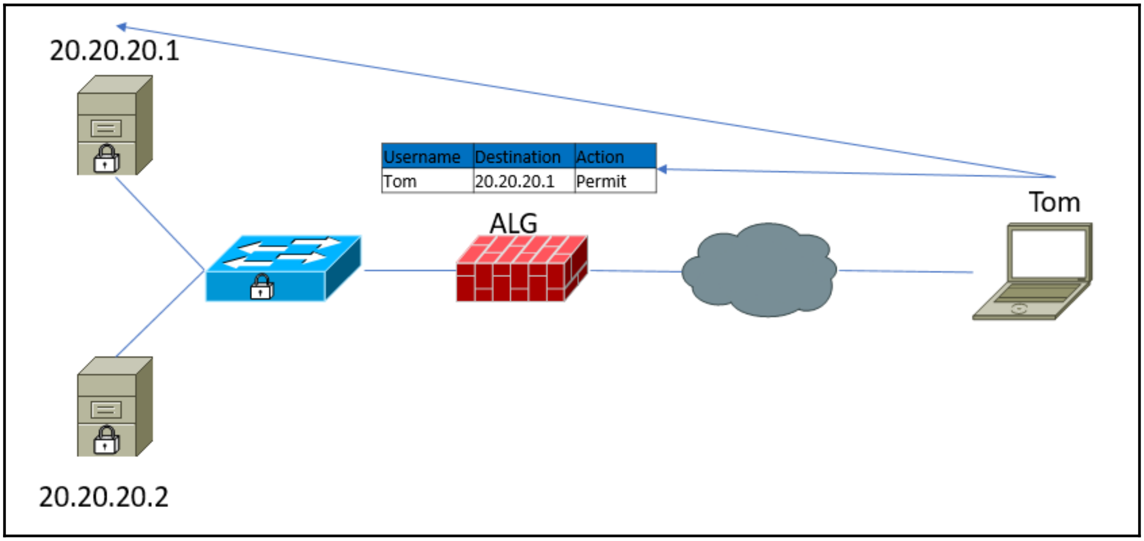
Multi Subnet Firewall Architecture


Internet
Perimeter Firewall
Web
Tier-1 Firewall
App
Tier-2 Firewall
Database

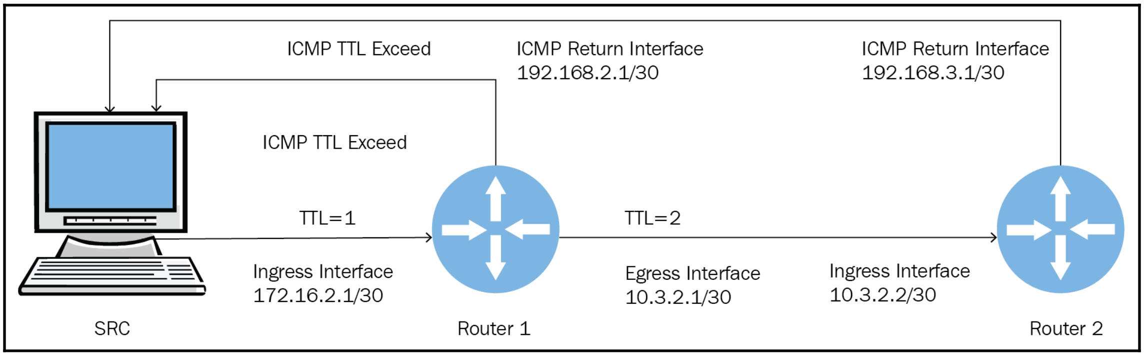

New Connection
Internet
Public IP – 2.2.2.2 Port 80
DMZ Firewall
Web
10.10.10.1
Tier-1 Firewall
App and DB
10.10.20.1

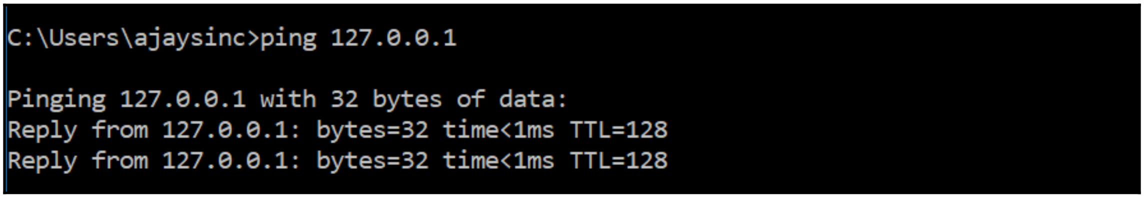

Host -1
Host -2
Application 7
Presentation 6
Session 5
Transport 4
Network 3
Data Link 2
Physical 1
Network
Data Link
Physical
Network
Data Link
Physical
Application 7
Presentation 6
Session 5
Transport 4
Network 3
Data Link 2
Physical 1


Application 7
Presentation 6
Session 5
Transport 4
Network 3
Data Link 2
Physical 1
Application 4
Transport 3
Network 2
Network Access Layer 1

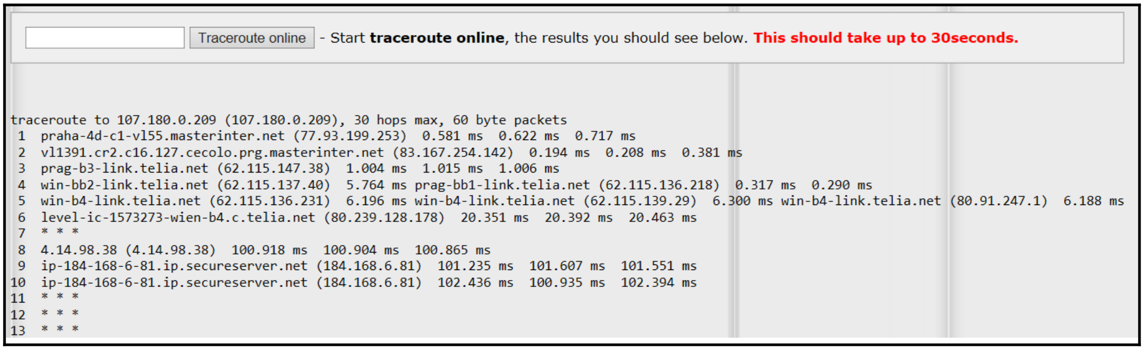


Username	Destination	Action
Tom	20.20.20.1	Permit



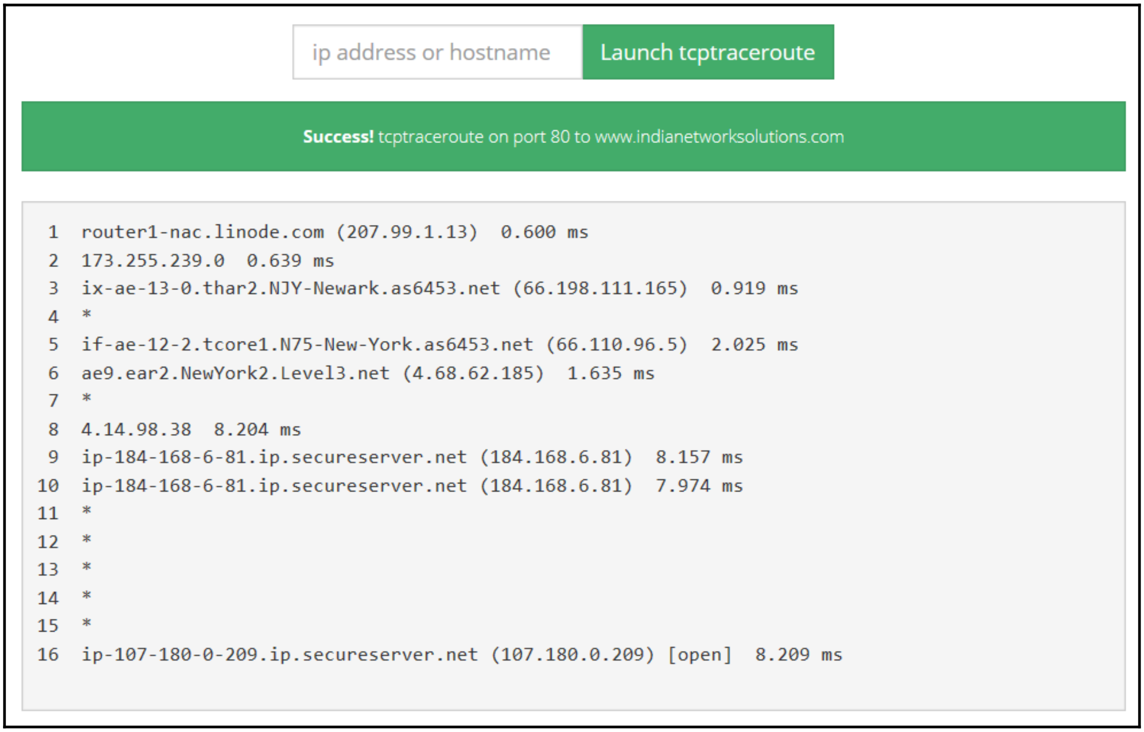


```
C:\Users\ajaysinc>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```



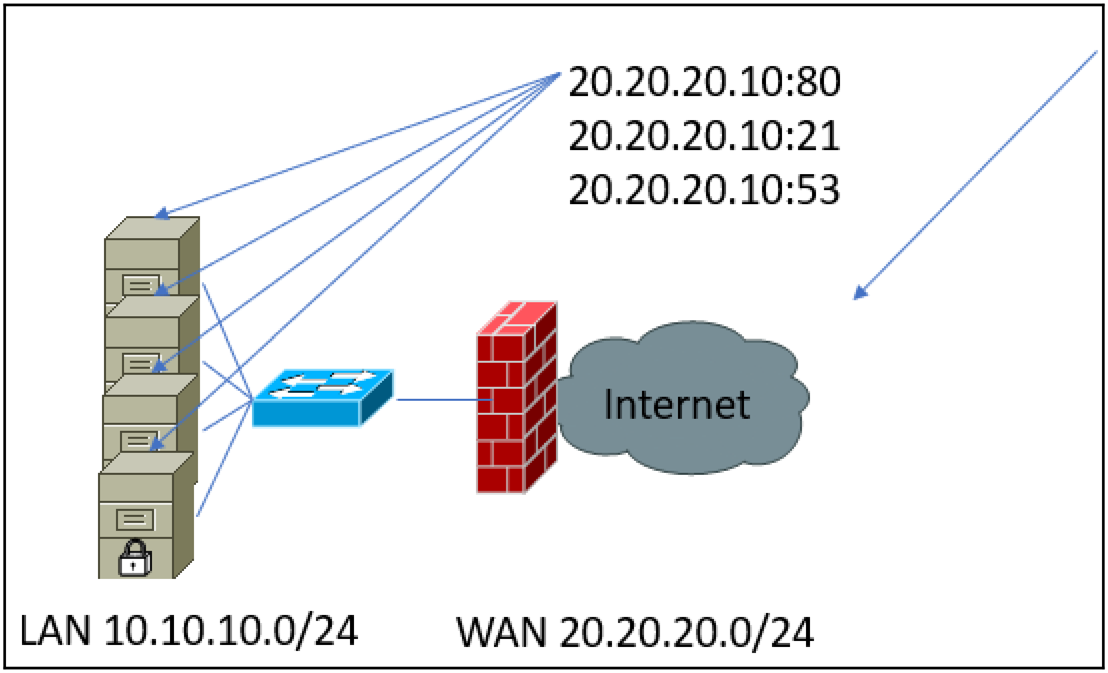
- Start **traceroute online**, the results you should see below. **This should take up to 30seconds.**

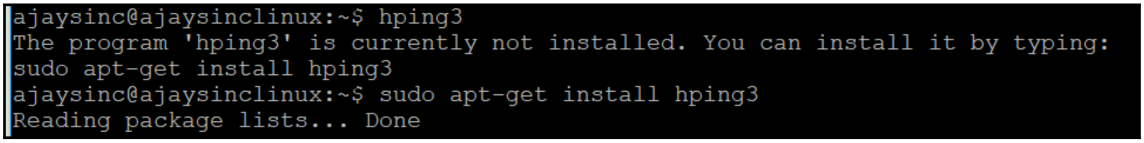
```
traceroute to 107.180.0.209 (107.180.0.209), 30 hops max, 60 byte packets
 1  praha-4d-c1-vl55.masterinter.net (77.93.199.253)  0.581 ms  0.622 ms  0.717 ms
 2  vl1391.cr2.c16.127.cecolo.prg.masterinter.net (83.167.254.142)  0.194 ms  0.208 ms  0.381 ms
 3  prag-b3-link.telia.net (62.115.147.38)  1.004 ms  1.015 ms  1.006 ms
 4  win-bb2-link.telia.net (62.115.137.40)  5.764 ms prag-bb1-link.telia.net (62.115.136.218)  0.317 ms  0.290 ms
 5  win-b4-link.telia.net (62.115.136.231)  6.196 ms win-b4-link.telia.net (62.115.139.29)  6.300 ms win-b4-link.telia.net (80.91.247.1)  6.188 ms
 6  level-ic-1573273-wien-b4.c.telia.net (80.239.128.178)  20.351 ms  20.392 ms  20.463 ms
 7  * * *
 8  4.14.98.38 (4.14.98.38)  100.918 ms  100.904 ms  100.865 ms
 9  ip-184-168-6-81.ip.secureserver.net (184.168.6.81)  101.235 ms  101.607 ms  101.551 ms
10  ip-184-168-6-81.ip.secureserver.net (184.168.6.81)  102.436 ms  100.935 ms  102.394 ms
11  * * *
12  * * *
13  * * *
```



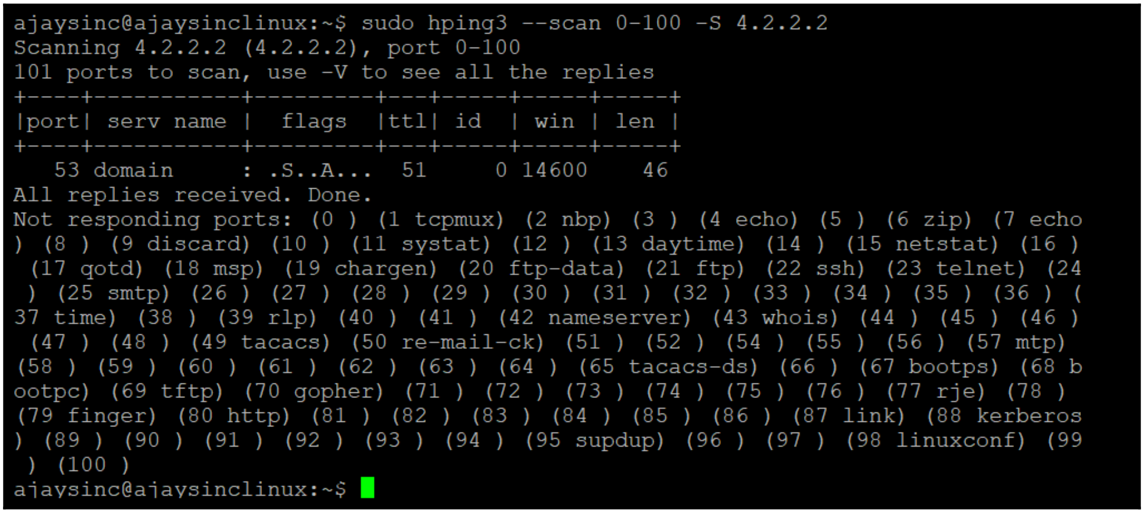
Success! tcptraceroute on port 80 to www.indianetworksolutions.com

```
 1  router1-nac.linode.com (207.99.1.13)  0.600 ms
 2  173.255.239.0  0.639 ms
 3  ix-ae-13-0.thar2.NJY-Newark.as6453.net (66.198.111.165)  0.919 ms
 4  *
 5  if-ae-12-2.tcore1.N75-New-York.as6453.net (66.110.96.5)  2.025 ms
 6  ae9.ear2.NewYork2.Level3.net (4.68.62.185)  1.635 ms
 7  *
 8  4.14.98.38  8.204 ms
 9  ip-184-168-6-81.ip.secureserver.net (184.168.6.81)  8.157 ms
10  ip-184-168-6-81.ip.secureserver.net (184.168.6.81)  7.974 ms
11  *
12  *
13  *
14  *
15  *
16  ip-107-180-0-209.ip.secureserver.net (107.180.0.209) [open]  8.209 ms
```

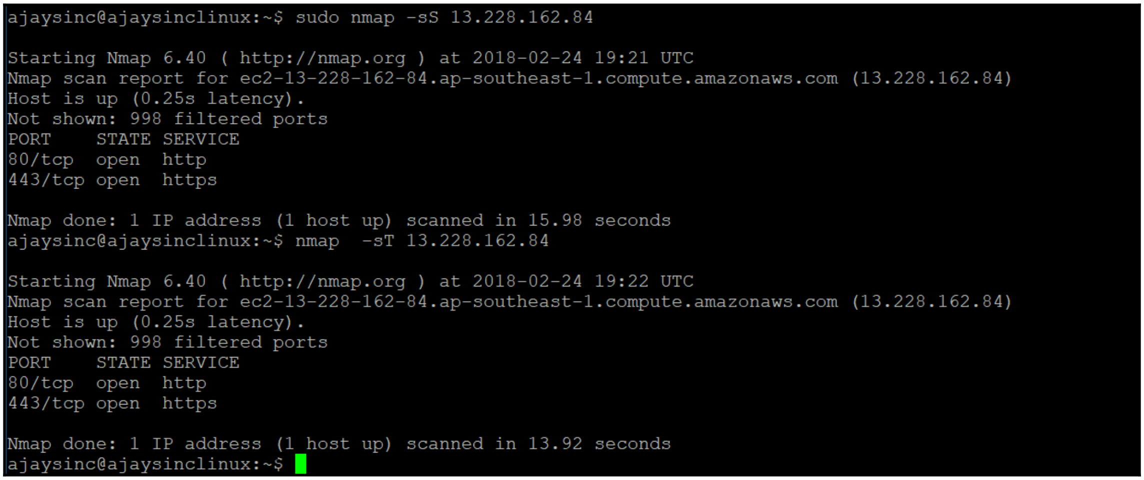




```
ajaysinc@ajaysinclinux:~$ hping3
The program 'hping3' is currently not installed. You can install it by typing:
sudo apt-get install hping3
ajaysinc@ajaysinclinux:~$ sudo apt-get install hping3
Reading package lists... Done
```

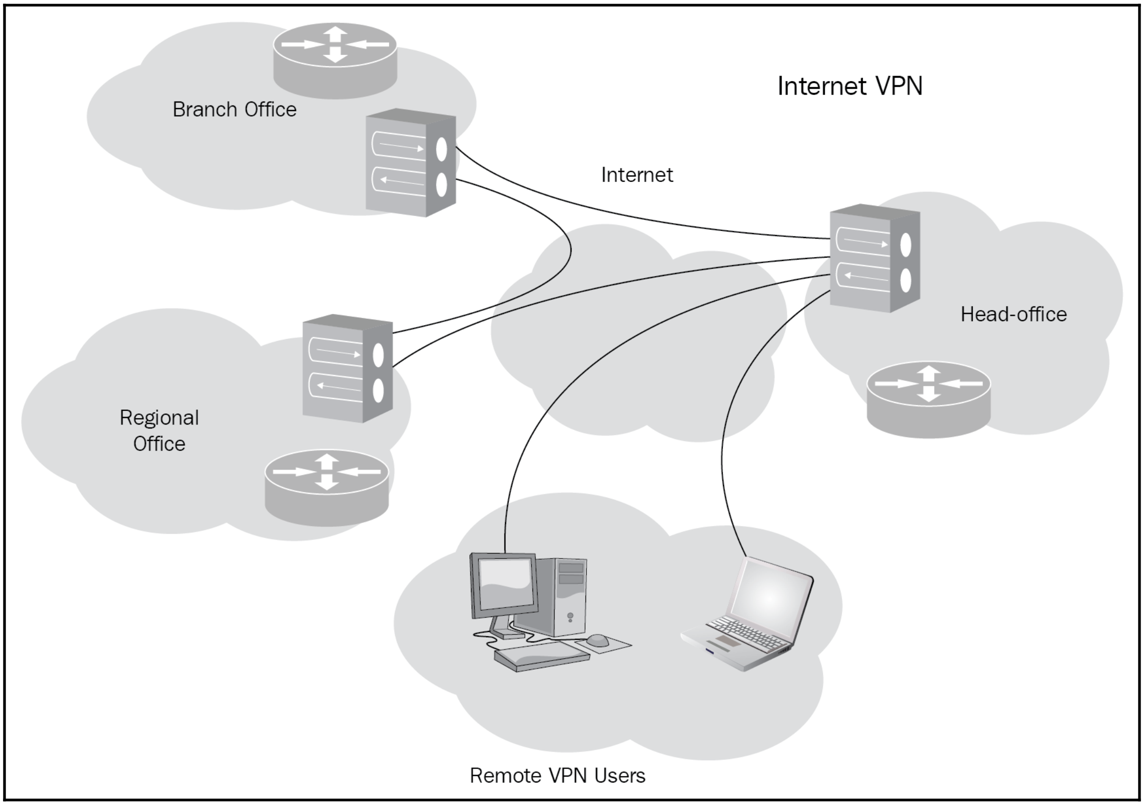


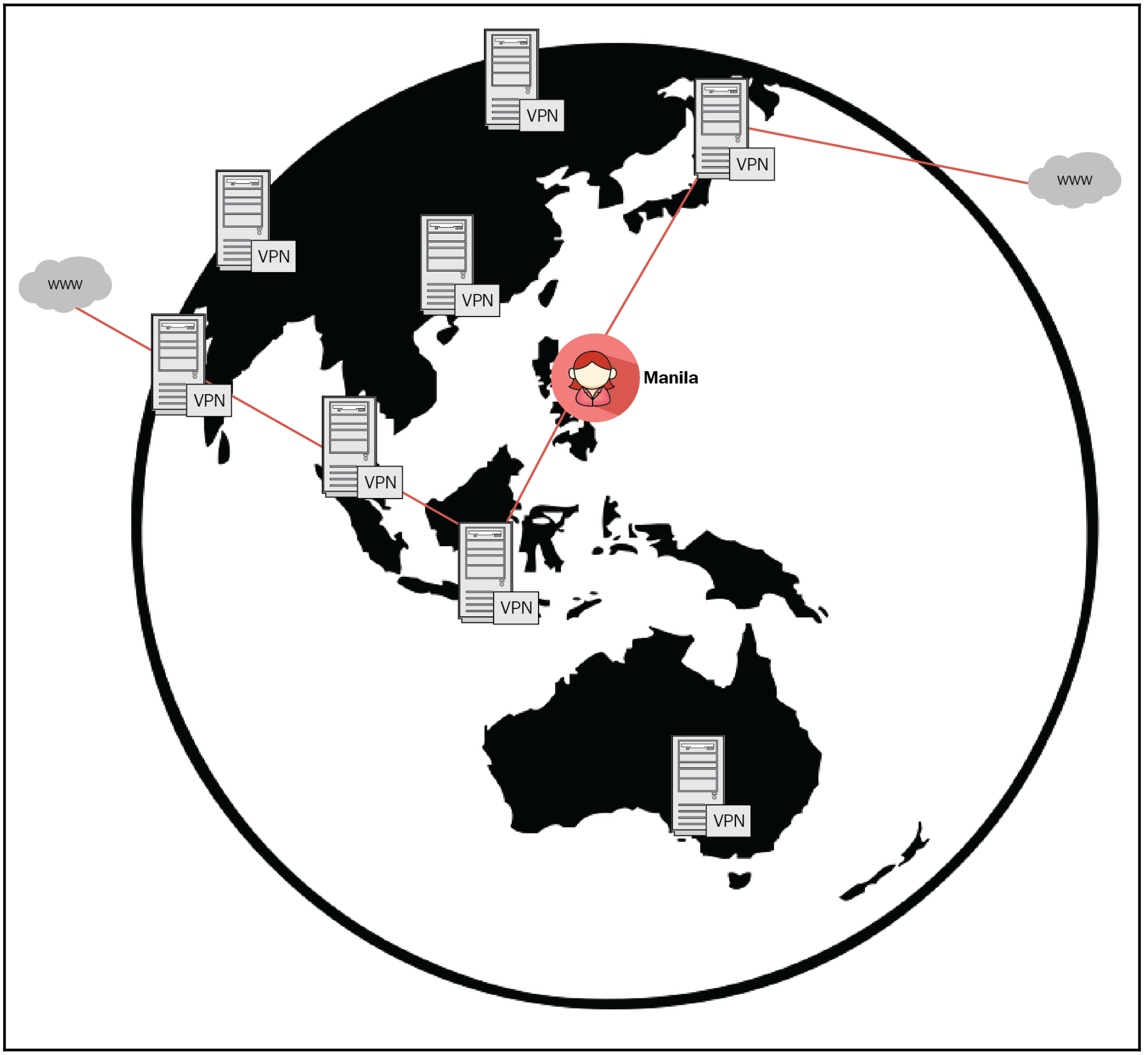
```
ajaysinc@ajaysinclinux:~$ sudo hping3 --scan 0-100 -S 4.2.2.2
Scanning 4.2.2.2 (4.2.2.2), port 0-100
101 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   53 domain     : .S..A...  51      0 14600    46
All replies received. Done.
Not responding ports: (0 ) (1 tcpmux) (2 nbp) (3 ) (4 echo) (5 ) (6 zip) (7 echo
) (8 ) (9 discard) (10 ) (11 systat) (12 ) (13 daytime) (14 ) (15 netstat) (16 )
 (17 qotd) (18 msp) (19 chargen) (20 ftp-data) (21 ftp) (22 ssh) (23 telnet) (24
 ) (25 smtp) (26 ) (27 ) (28 ) (29 ) (30 ) (31 ) (32 ) (33 ) (34 ) (35 ) (36 ) (
37 time) (38 ) (39 rlp) (40 ) (41 ) (42 nameserver) (43 whois) (44 ) (45 ) (46 )
 (47 ) (48 ) (49 tacacs) (50 re-mail-ck) (51 ) (52 ) (54 ) (55 ) (56 ) (57 mtp)
(58 ) (59 ) (60 ) (61 ) (62 ) (63 ) (64 ) (65 tacacs-ds) (66 ) (67 bootps) (68 b
ootpc) (69 tftp) (70 gopher) (71 ) (72 ) (73 ) (74 ) (75 ) (76 ) (77 rje) (78 )
(79 finger) (80 http) (81 ) (82 ) (83 ) (84 ) (85 ) (86 ) (87 link) (88 kerberos
) (89 ) (90 ) (91 ) (92 ) (93 ) (94 ) (95 supdup) (96 ) (97 ) (98 linuxconf) (99
 ) (100 )
ajaysinc@ajaysinclinux:~$
```

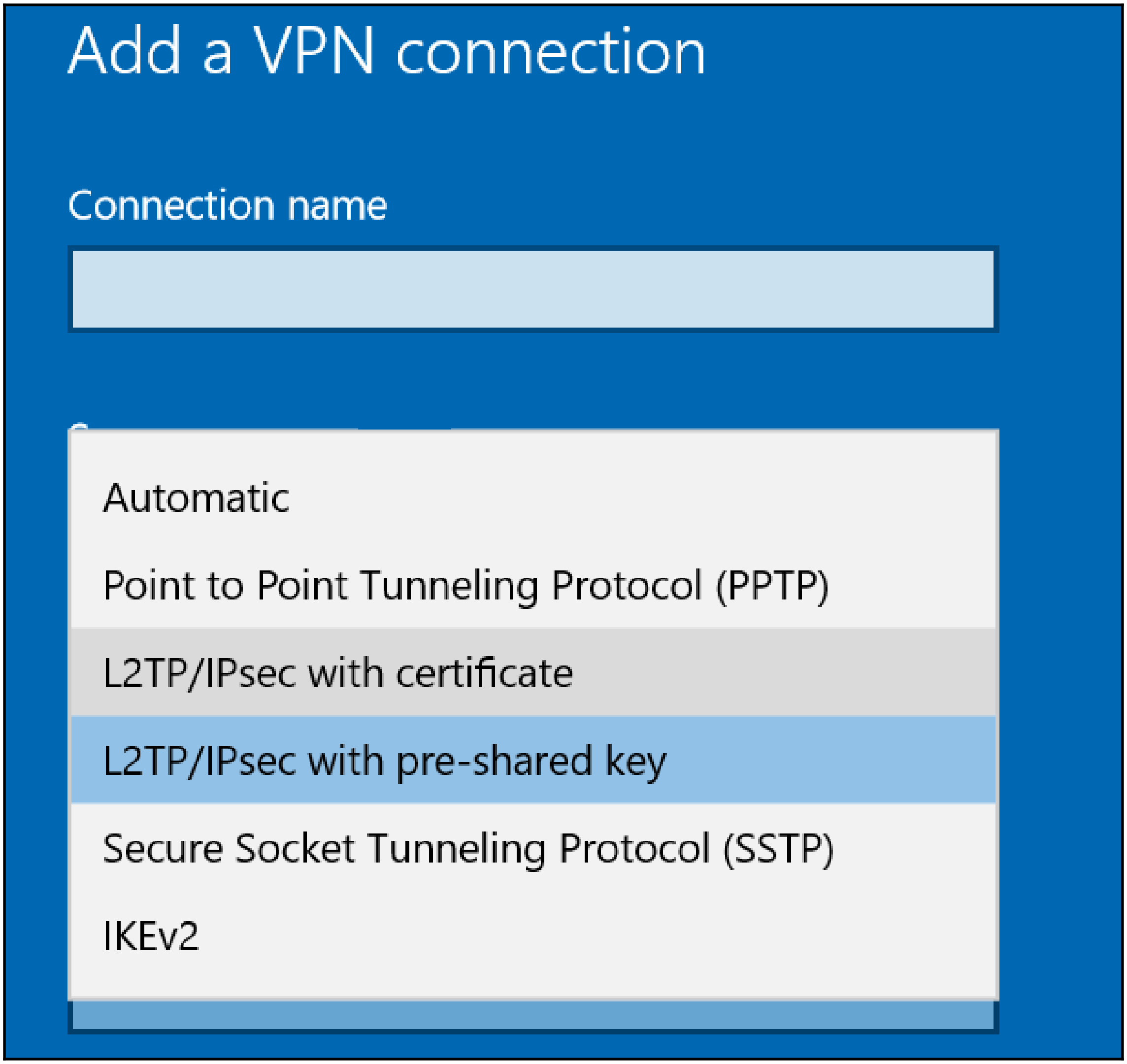


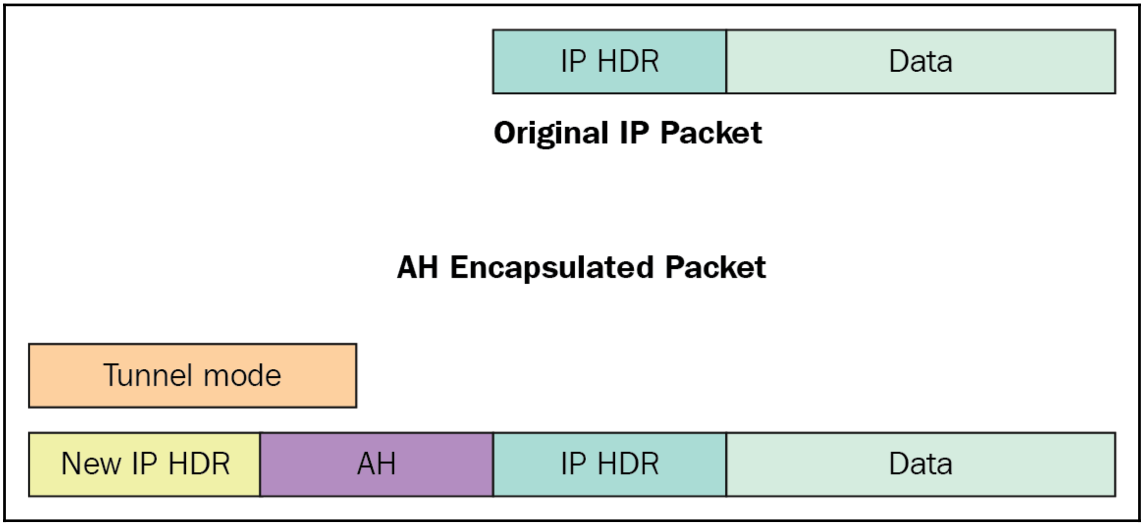
```
ajaysinc@ajaysinclinux:~$ sudo nmap -sS 13.228.162.84

Starting Nmap 6.40 ( http://nmap.org ) at 2018-02-24 19:21 UTC
Nmap scan report for ec2-13-228-162-84.ap-southeast-1.compute.amazonaws.com (13.228.162.84)
Host is up (0.25s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 15.98 seconds
ajaysinc@ajaysinclinux:~$ nmap  -sT 13.228.162.84

Starting Nmap 6.40 ( http://nmap.org ) at 2018-02-24 19:22 UTC
Nmap scan report for ec2-13-228-162-84.ap-southeast-1.compute.amazonaws.com (13.228.162.84)
Host is up (0.25s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 13.92 seconds
ajaysinc@ajaysinclinux:~$
```

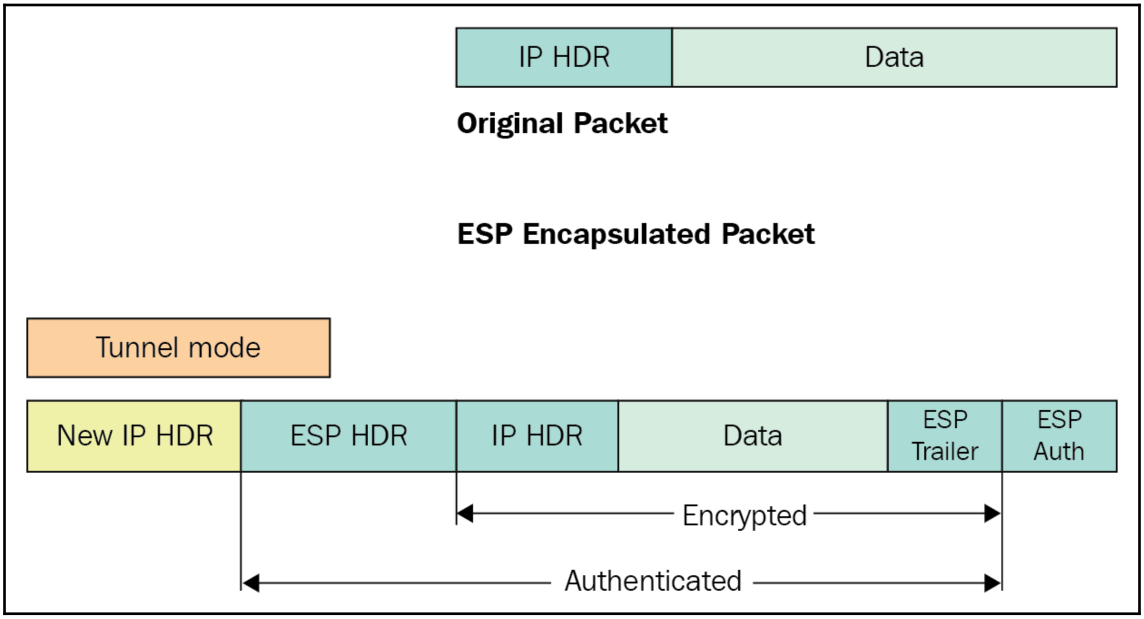
Chapter 11: VPN & WAN Encryption

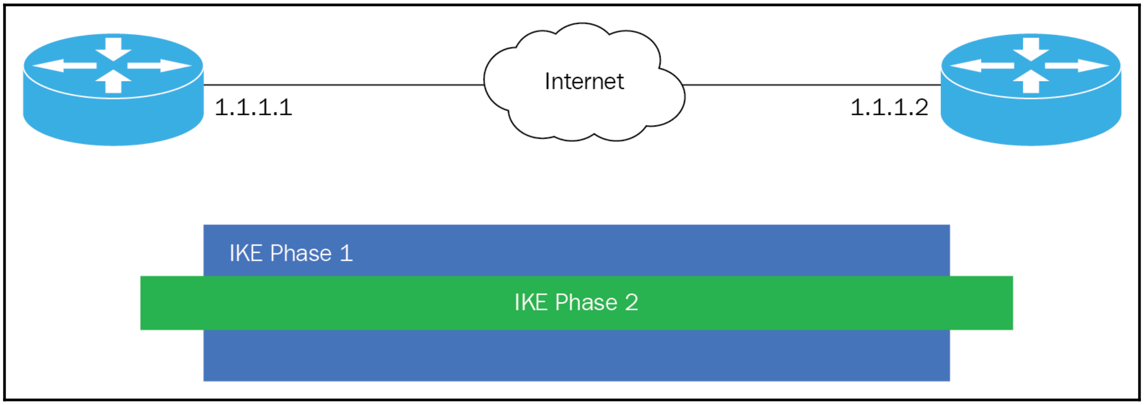


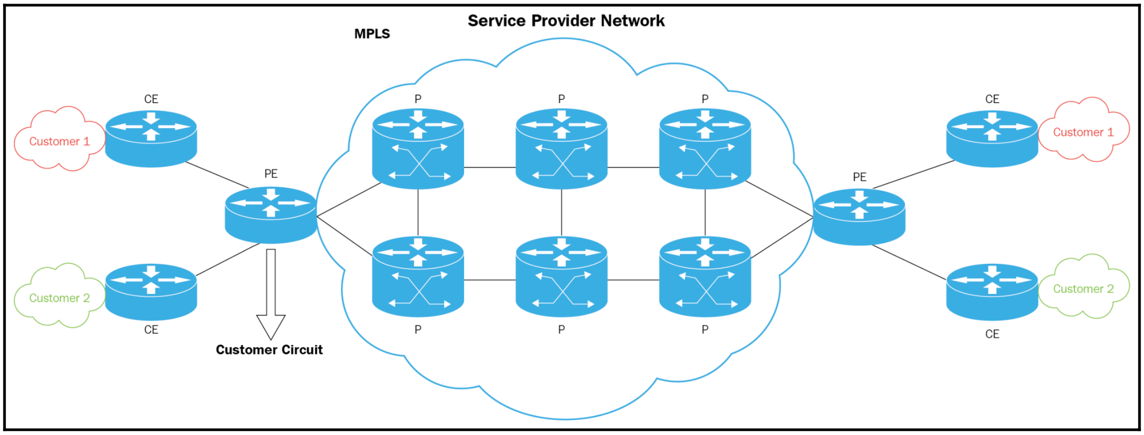

VPN
VPN
VPN
VPN
www
VPN
VPN
Manila
VPN
www
VPN
VPN

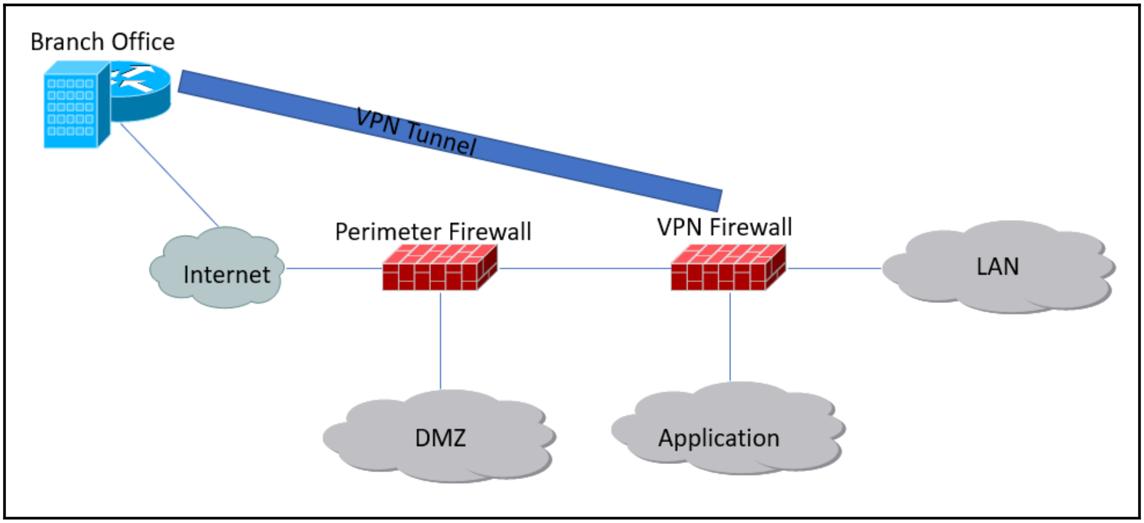

Add a VPN connection
Connection name
Automatic
Point to Point Tunneling Protocol (PPTP)
L2TP/IPsec with certificate
L2TP/IPsec with pre-shared key
Secure Socket Tunneling Protocol (SSTP)
IKEv2

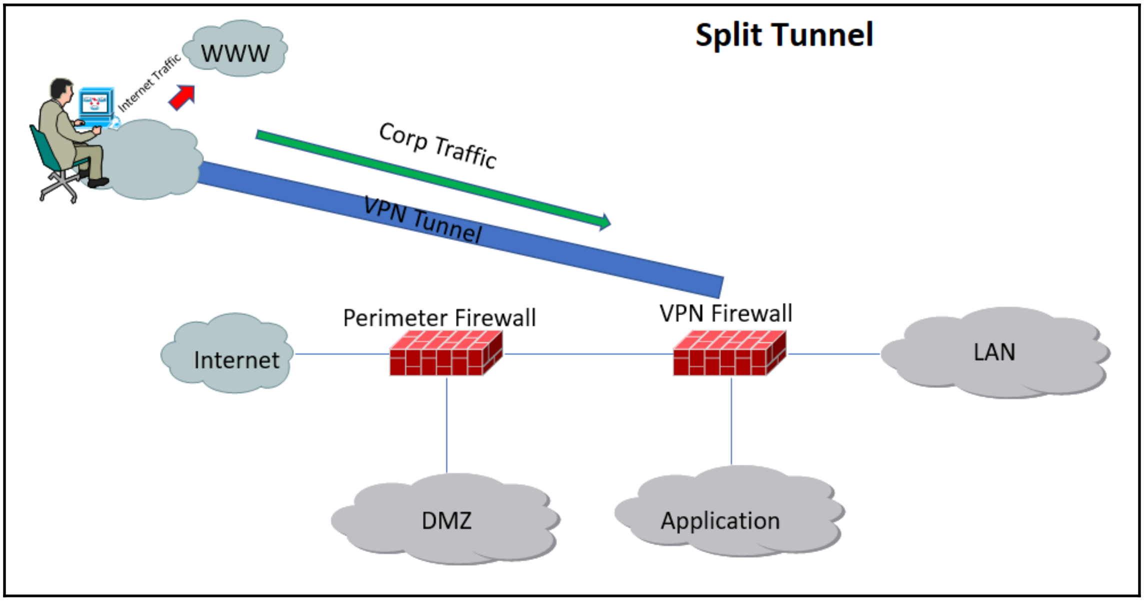

IP HDR
Data
Original IP Packet
AH Encapsulated Packet
Tunnel mode
New IP HDR
AH
IP HDR
Data

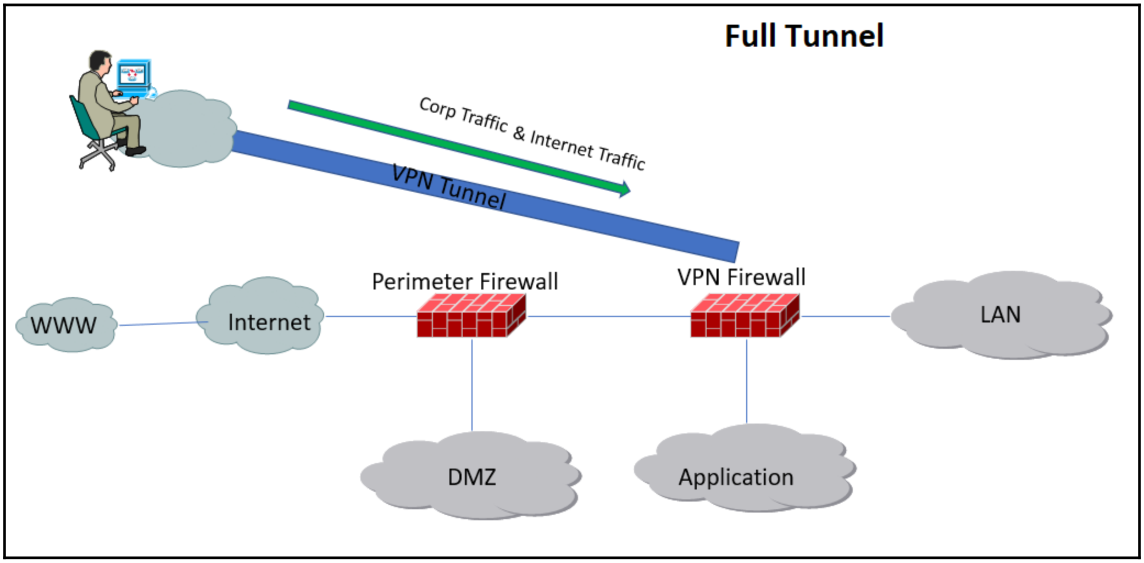

IP HDR
Data
Original Packet
ESP Encapsulated Packet
Tunnel mode
New IP HDR
ESP HDR
IP HDR
Data
ESP Trailer
ESP Auth
Encrypted
Authenticated

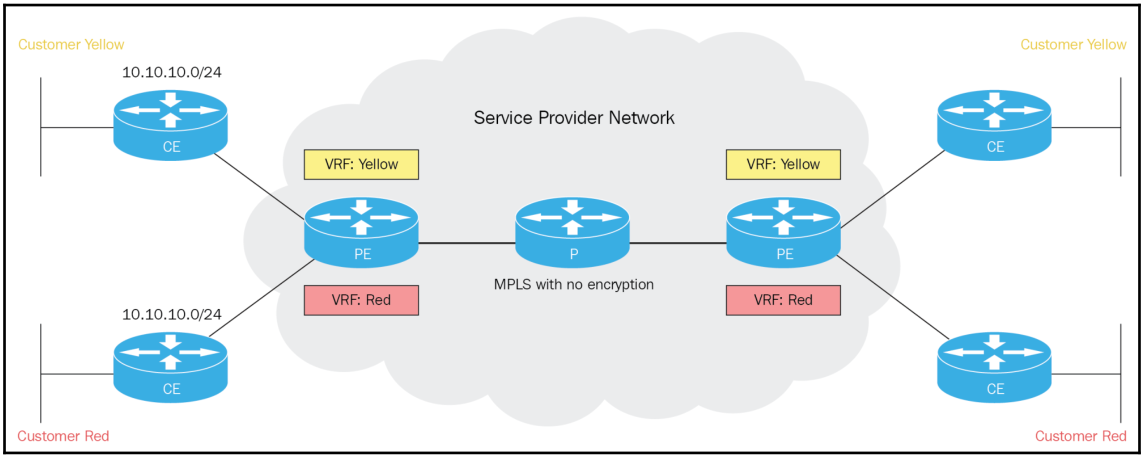

Internet
1.1.1.1
1.1.1.2
IKE Phase 1
IKE Phase 2

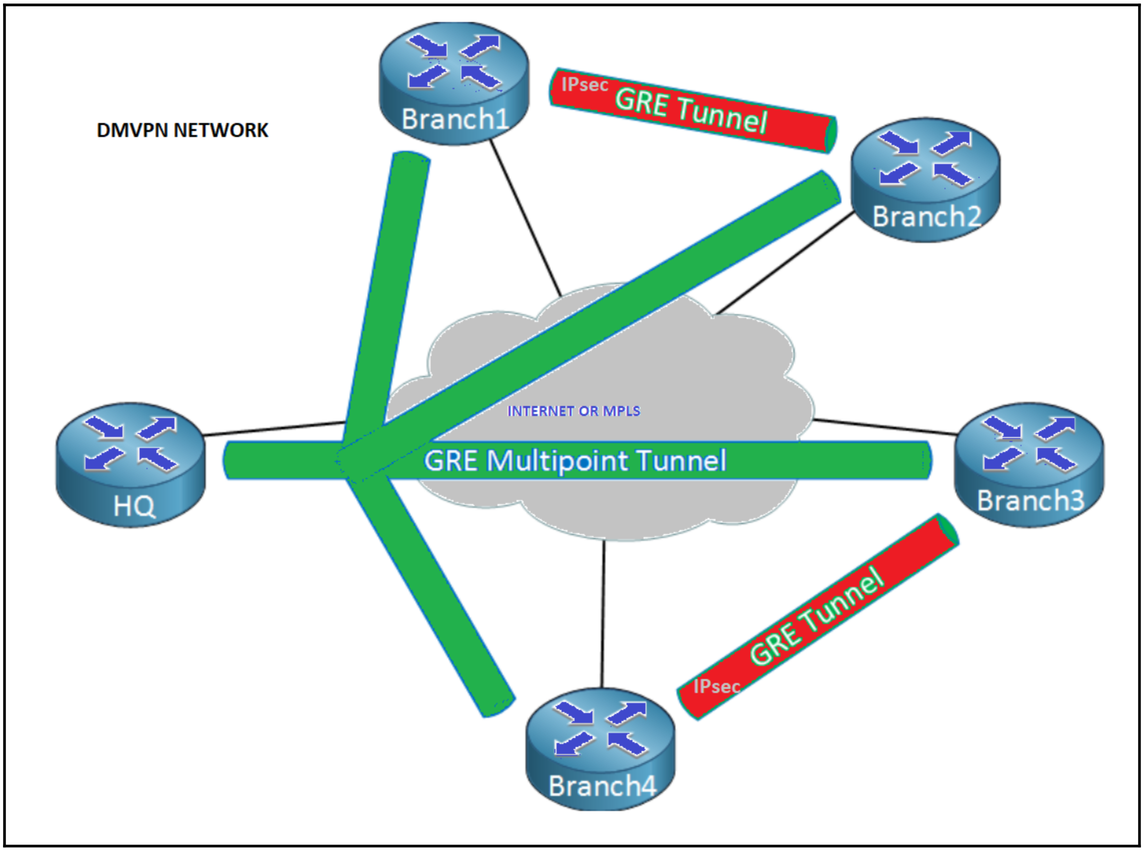

Service Provider Network
MPLS
CE
Customer 1
PE
P
P
P
PE
CE
Customer 1
Customer 2
CE
P
P
P
Customer Circuit
Customer 2
CE


Branch Office
VPN Tunnel
Perimeter Firewall
VPN Firewall
Internet
LAN
DMZ
Application

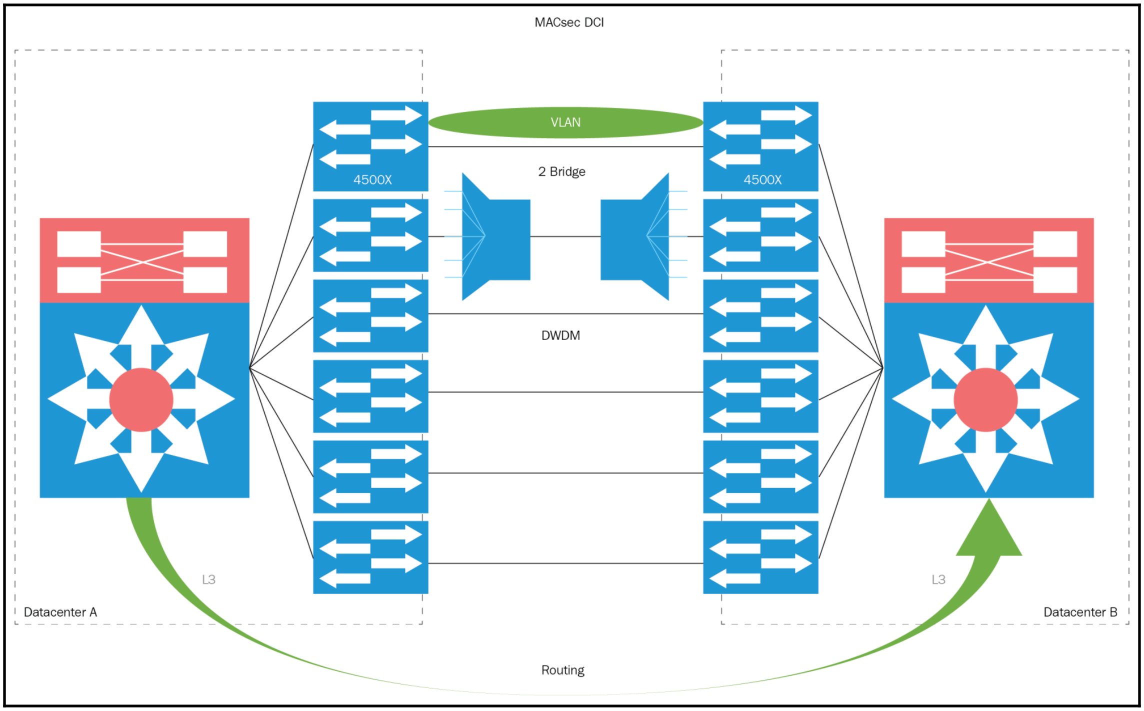

Split Tunnel
WWW
Internet Traffic
Corp Traffic
VPN Tunnel
Perimeter Firewall
VPN Firewall
Internet
LAN
DMZ
Application

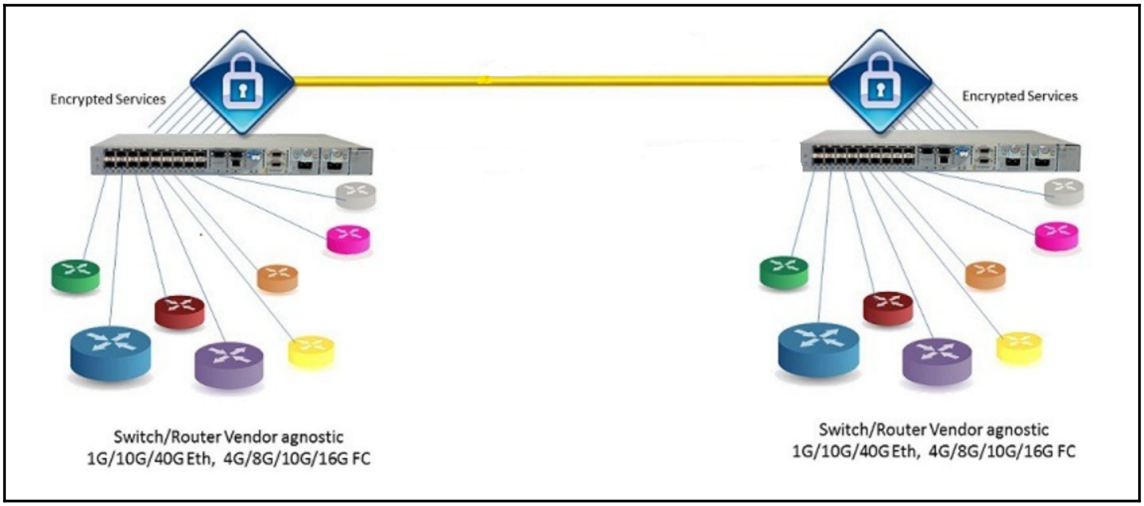

Full Tunnel
Corp Traffic & Internet Traffic
VPN Tunnel
Perimeter Firewall
VPN Firewall
WWW
Internet
LAN
DMZ
Application


Customer Yellow
Customer Yellow
10.10.10.0/24
Service Provider Network
CE
CE
VRF: Yellow
VRF: Yellow
PE
P
PE
MPLS with no encryption
VRF: Red
VRF: Red
10.10.10.0/24
CE
CE
Customer Red
Customer Red

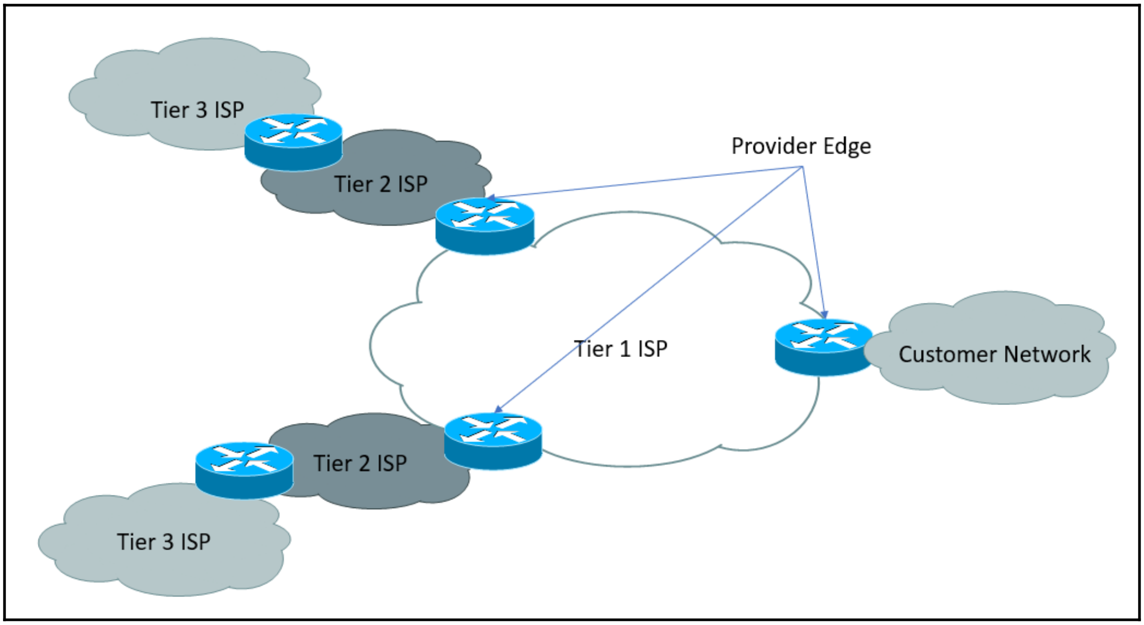


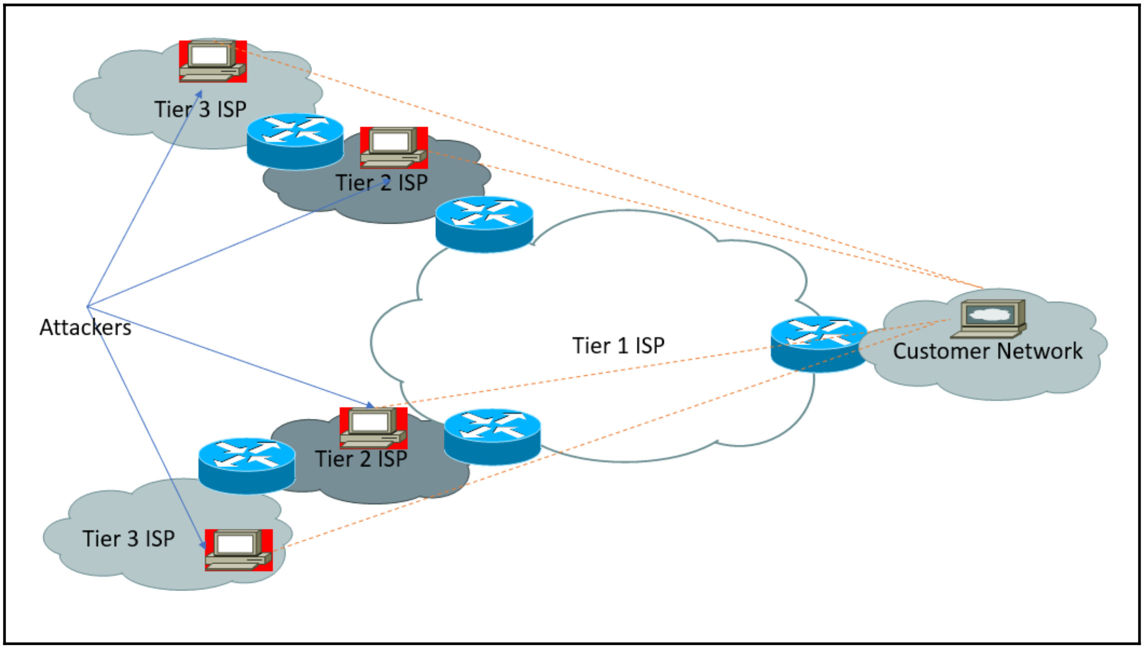
DMAC	SMAC	802.1AE Header	802.1Q	CMD	ETYPE	PAYLOAD	ICV	CRC
					ENCRYPTED			

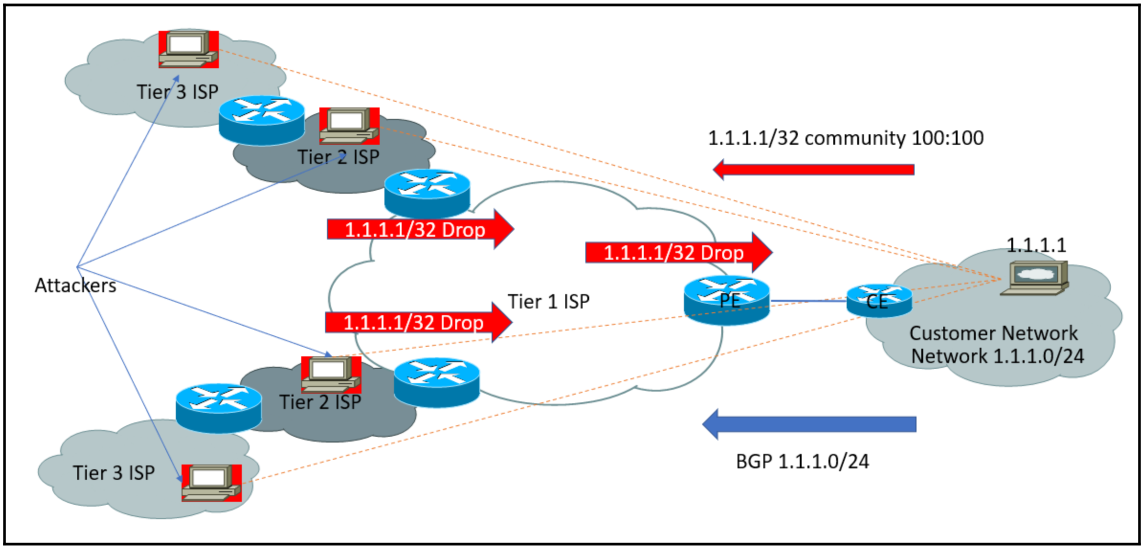

MACsec DCI
VLAN
2 Bridge
4500X
4500X
DWDM
L3
L3
Datacenter A
Datacenter B
Routing

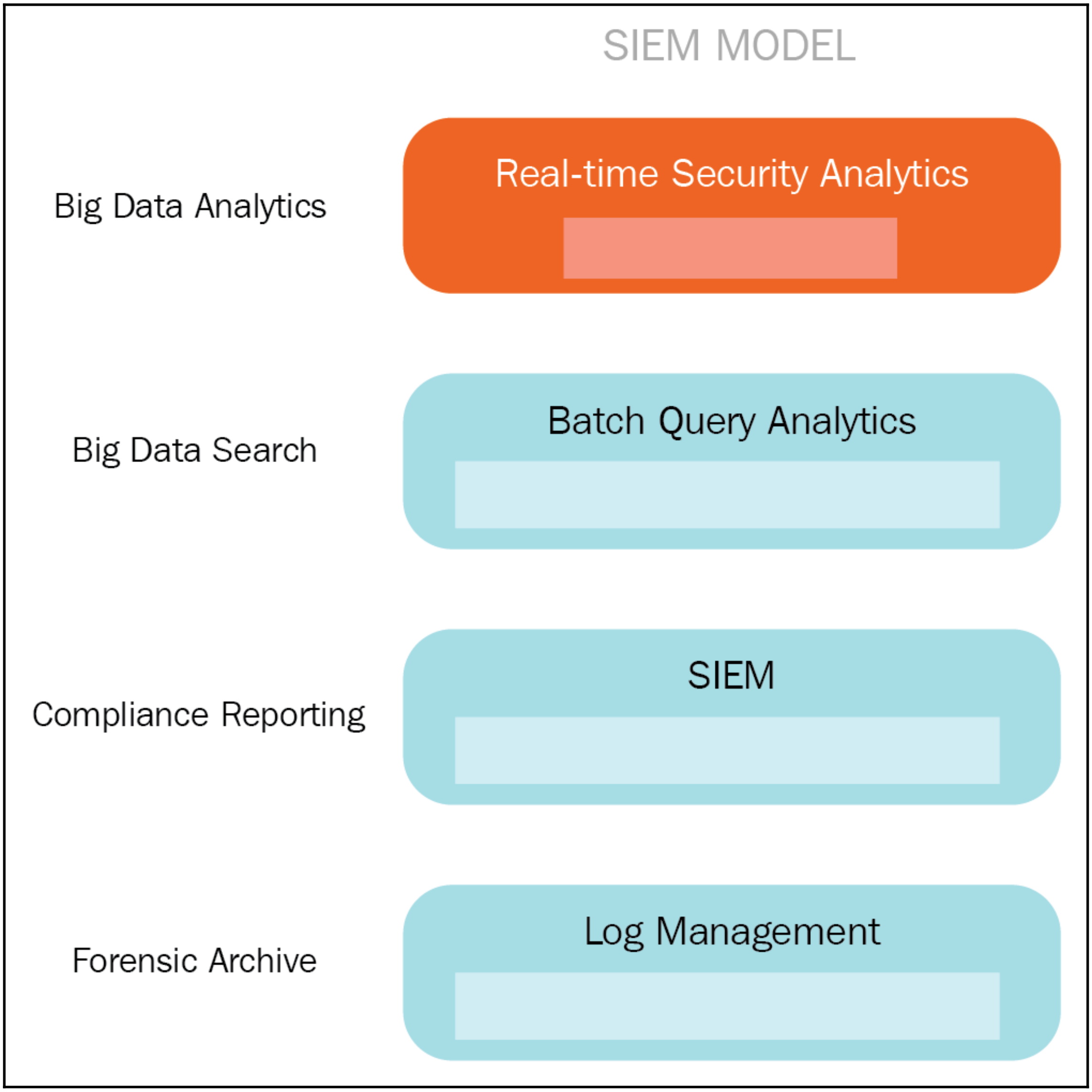

Encrypted Services
Encrypted Services
Switch/Router Vendor agnostic
1G/10G/40G Eth, 4G/8G/10G/16G FC
Switch/Router Vendor agnostic
1G/10G/40G Eth, 4G/8G/10G/16G FC

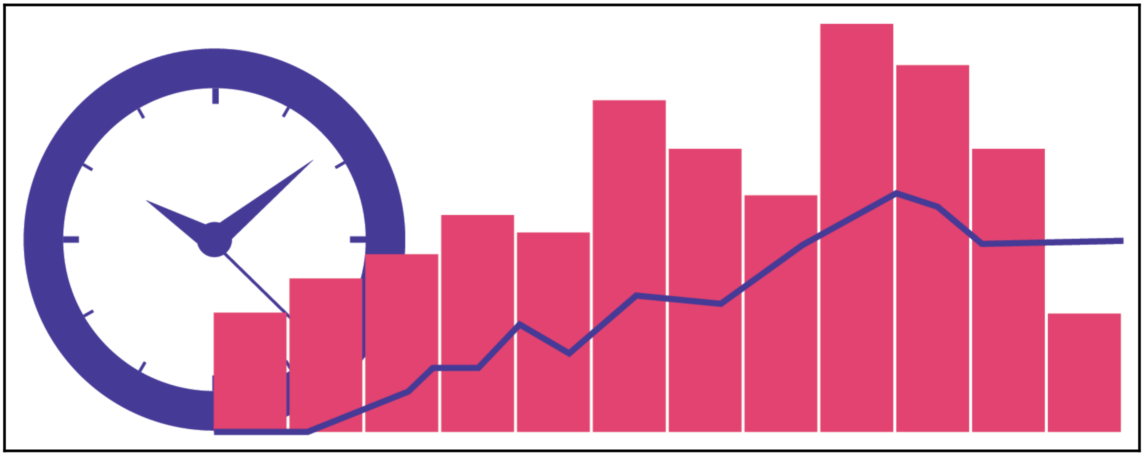
Chapter 12: Summary and Scope of Security technologies

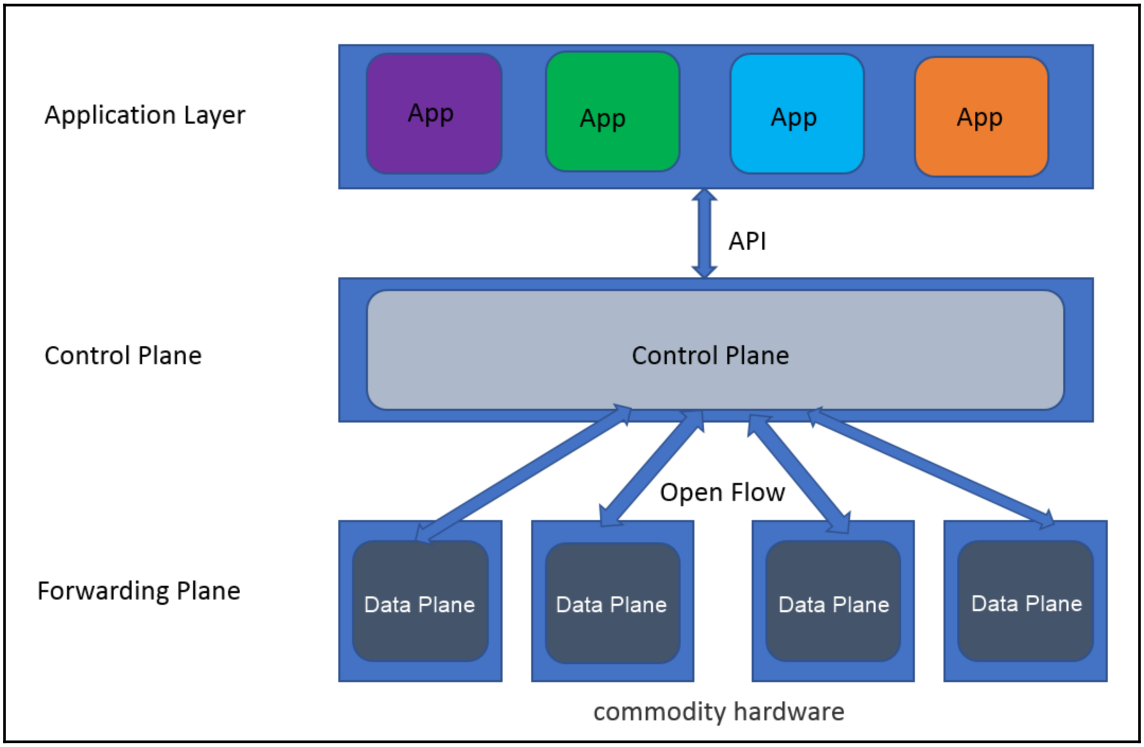


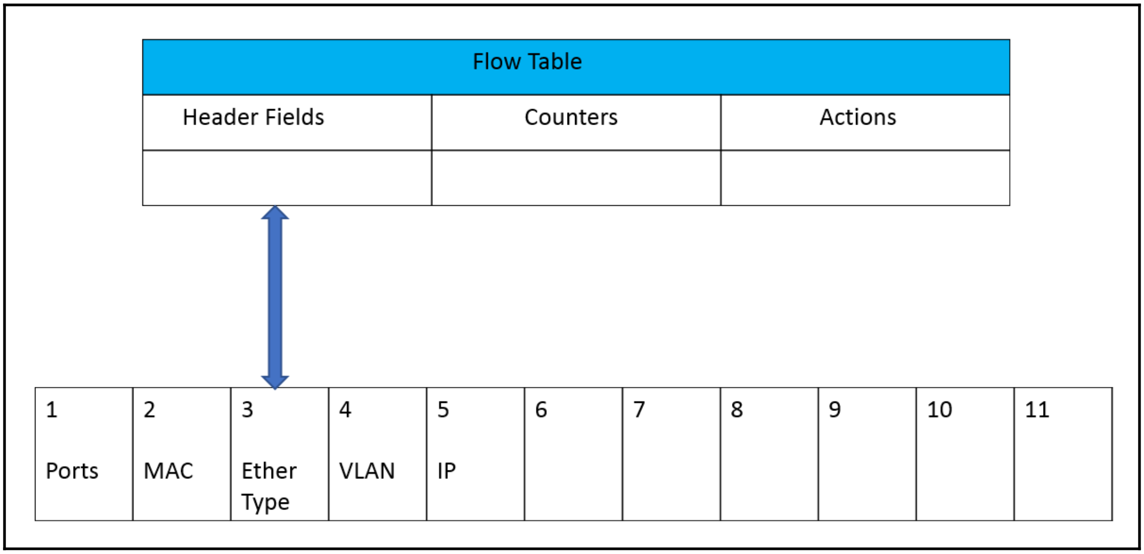

Tier 3 ISP
Tier 2 ISP
Attackers
Tier 1 ISP
Customer Network
Tier 2 ISP
Tier 3 ISP


Tier 3 ISP
Tier 2 ISP
1.1.1.1/32 community 100:100
1.1.1.1/32 Drop
1.1.1.1/32 Drop
1.1.1.1
Attackers
Tier 1 ISP
PE
CE
1.1.1.1/32 Drop
Customer Network
Network 1.1.1.0/24
Tier 2 ISP
Tier 3 ISP
BGP 1.1.1.0/24


SIEM MODEL
Big Data Analytics
Real-time Security Analytics
Big Data Search
Batch Query Analytics
Compliance Reporting
SIEM
Forensic Archive
Log Management

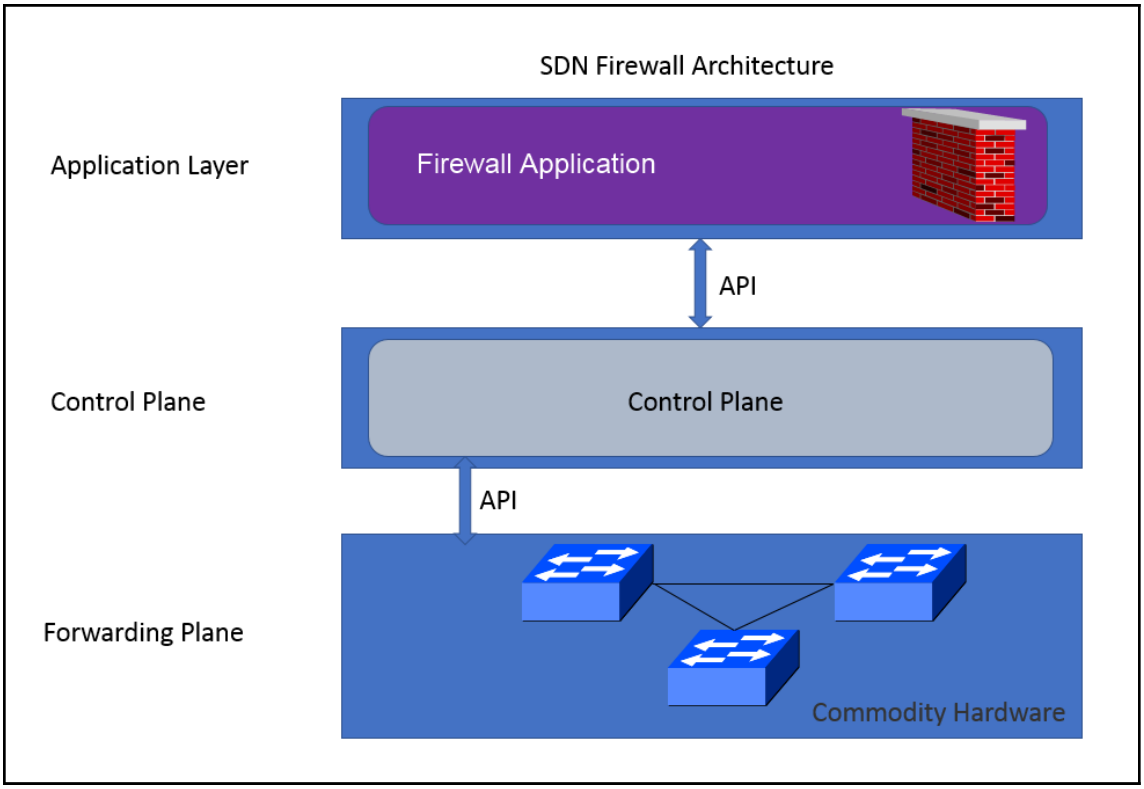



Application Layer
App
App
App
App
API
Control Plane
Control Plane
Open Flow
Forwarding Plane
Data Plane
Data Plane
Data Plane
Data Plane
commodity hardware

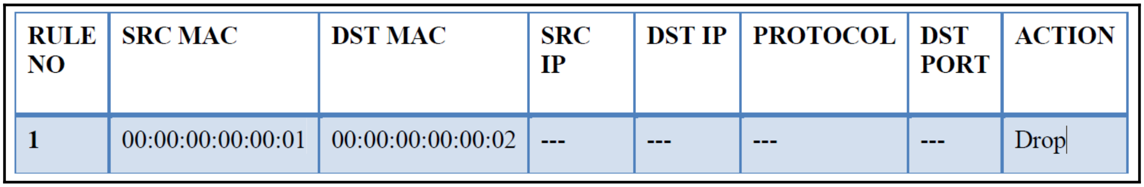


Flow Table		
Header Fields	Counters	Actions

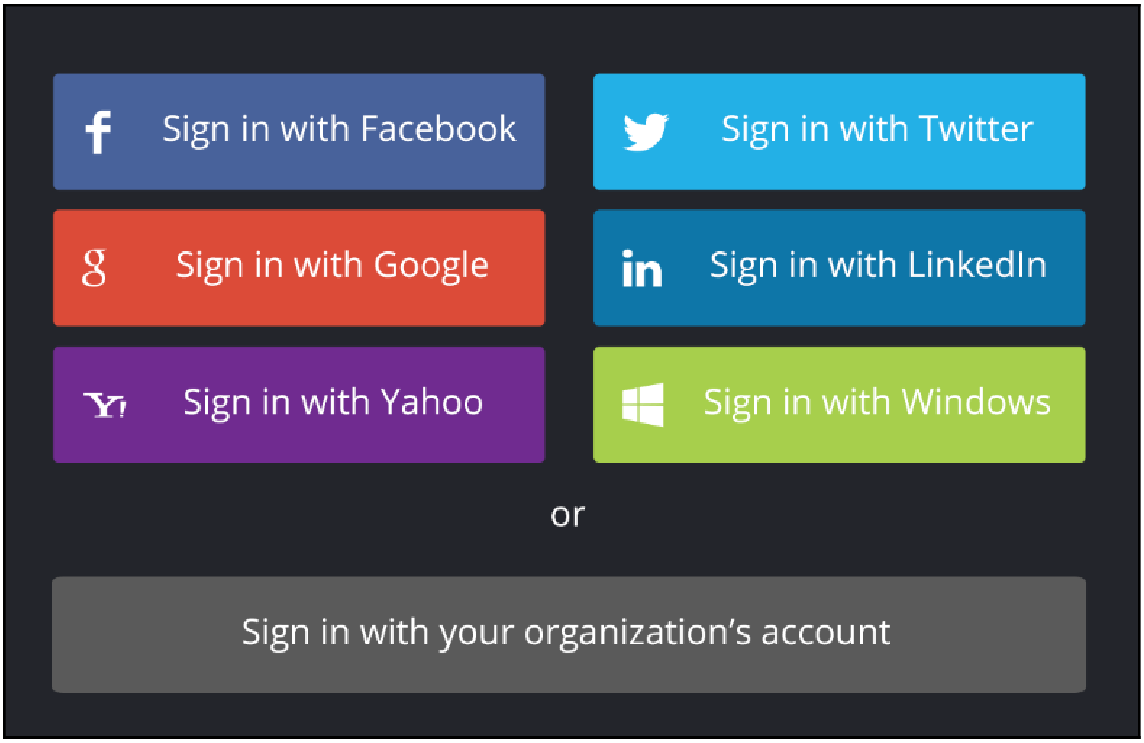
1	2	3	4	5	6	7	8	9	10	11
Ports	MAC	Ether Type	VLAN	IP						



SDN Firewall Architecture



RULE NO	SRC MAC	DST MAC	SRC IP	DST IP	PROTOCOL	DST PORT	ACTION
1	00:00:00:00:00:01	00:00:00:00:00:02	---	---	---	---	Drop


Sign in with Facebook
Sign in with Twitter
Sign in with Google
Sign in with LinkedIn
Sign in with Yahoo
Sign in with Windows
or
Sign in with your organization’s account