Network Security with Firewalls (IOS, ASA, Juniper, Paloalto and Checkpoint)

Detailed Syllabus

A firewall is like a security guard standing at the gate trying to give security for an enterprise network connected to Internet. It tries to protect the enterprise's network from attacks, from the Internet.

To make the students understand the concepts of network security in-depth with practical experience, we at Koti Concepts train the students on a real time case study.

About the case study

The case study is designed with 96 routers, 254 systems and around 30 firewalls keeping in mind to create conditions that prevail in real time enterprise networks.

The case study is divided into 4 autonomous systems managed by their respective service providers. Different companies like Pumpkin, Apple, Mango, Lemon, Coconut, Tomato, Potato, Brinjal, Cabbage, Cucumber, Ginger, Banana, Carrot, and Orange connect to the Internet in the case study with their network resources in the head and branch offices. These companies to protect their resources from hacker attacks, deploy a firewall between their respective companies'networks and the Internet. The following table shows the companies with their respective firewall solutions.

S. No	Name of the Company	Firewall used	Remarks
1	Pumpkin	IOS	Head office with 2 branch offices
2	Apple	ASA	Head office with 2 branch offices
3	Lemon	Juniper	Head office with 2 branch offices
4	Coconut	Paloalto	Head office with 2 branch offices
5	Mango	Checkpoint	Only Head office
6	Tomato	Checkpoint	Head office with 2 branch offices
7	Orange	Checkpoint	Head office with 2 branch offices
8	Banana	IOS	Head office with 2 branch offices
9	Carrot	IOS	Head office with 2 branch offices

10	Potato Brinjal Cabbage	Checkpoint	Head office with virtualization on Checkpoint VSX gateway
11	Cucumber	Checkpoint	Head office with Cluster-XL Cluster
12	Ginger	Checkpoint	Head office with VRRP Cluster

Internet clients and servers in the case study

The users in the above companies would like to access the Servers on the Internet for various services like DNS, HTTP, FTP and SMTP. Likewise, the users on the Internet would like to access the servers in the networks of the above companies. The firewalls in the respective companies should be configured with NAT and security policies to allow access. To practise on the above configuration labs, the following systems running different services are designed in the case study.

S.No	Name of the Company	Services	Remarks
1	ABC	www.abc.com ftp.abc.com abc-mail-server	ABC company's servers
2	XYZ	www.xyz.com ftp.xyz.com xyz-mail-server	XYZ company's servers
3	Yahoo	Yahoo.com Mail-server	Yahoo mail server
3	Gmail	Gmail.com Mail-server	Gmail mail server
4	Go Mummy	Go Mummy CA-Server Mail-server	GoMummy.com Certificate Authority
5	Internet Clients	HTTP, FTP, POP3, IMAP, SMTP Clients	Client desktops to access various services running on the Internet and in the various companies

Description of the different company's networks in the case study

The organizations listed above(Pumpkin, Apple, Mango, Lemon, Coconut, Tomato, Potato, Brinjal, Cabbage, Cucumber, Ginger, Banana, Carrot, and Orange) have HTTP servers, FTP servers and Mail servers present in their DMZ networks which are accessed by the Internet clients. The users of these companies also would like to access the servers on the Internet. The users of the above organizations also would like to access the resources present in their head office, branch offices and business partner's network.

The appropriate systems running different services are deployed in the networks of all the above mentioned companies in the case study

Training methodology and Lab facilities

All the concepts described in the syllabus are explained and demonstrated by the trainer at packet level. The students do the lab practice then and there in the classroom. Each and every student is provided with an IBM server with 32 GB RAM, 4 TB hard disk, Xeon processor, and 28-inch monitor. The VMs with the relevant applications installed are copied for all the students in their individual servers. Each and every student can practice on his own dedicated case study setup, accessing all the 96 routers, 254 servers and 30 firewalls.

A detailed manual with the configuration tasks is provided to the students to practice on the concepts taught in the class then and there.

About the trainer

All the classes at Koti Concepts are conducted by Koti. He has around 20 years experience in teaching networking courses. He is the founder chairman of the most popular "Sans Bound Solutions Private Limited", a networking training institute at Chennai.

Course content and flow

Chapter no 1: Configuration of IP routing on the routers in the case study diagram so that the various customers networks connected to the 4 different ISPs could communicate with each other

Concepts learnt and practised:

1. Configuration of routers with routing protocols like RIP, EIGRP, OSPF, IS-IS and BGP
2. Static routing and the default routes
3. Redistribution between the routing protocols and solution to the associated issues

Chapter no 2: Configuration of the ISP-DNS server with various "hosts" records and "MX" records so that the client systems on the Internet could access various HTTP, FTP, POP3, IMAP, and SMTP servers on the Internet.

Concepts learnt and practised:

1. Configuration of the ISP-DNS server with a zone, domain and various records like "host" and "MX" records
2. Configuration of mail boxes for different users in their relevant mail servers

3. Configuration of outlook express as email-client for different users
4. Understanding the process and configuration steps involved in sending and receiving the mails between users in different organizations.

Chapter no 3: Configuration of the IOS firewall of Pumpkin Head office with NAT and Access-lists

Concepts learnt and practised:

1. Configuration of dynamic NAT on Pumpkin IOS firewall with and without overload, so that the users of Pumpkin head office could access the DNS, HTTP, FTP and SMTP servers on the internet. Configuration of NAT pools
2. Configuration of static NAT on Pumpkin IOS firewall so that users on the Internet could access the HTTP, FTP and SMTP servers in the DMZ network of Pumpkin head office.
3. Configuration of standard and extended access-lists considering the traffic flow patterns
4. Understanding the structure of the following packets
    a. TCP 3-way handshake packets during connection establishment and TCP connection termination packets, TCP flags like SYN, ACK, RESET, PUSH, URGENT and FIN
    b. DNS query and DNS query response UPD protocol packets
    c. HTTP get request and response
    d. FTP control session, FTP data session in active mode, FTP data session in passive mode
    e. ICMP echo request, ICMP echo reply, ICMP destination host is unreachable, ICMP communication administratively prohibited and destination port is unreachable
    f. POP3, IMAP and SMTP protocol packets
5. Configuration of access-lists considering the pre-nat and post-nat interfaces.

Chapter no 4: Configuration of the ASA firewall of Apple Head office with NAT and Access-lists

Concepts learnt and practised:

1. Configuration of security policies on ASA firewall to allow different network traffic according to the specification
2. Configuration of dynamic NAT on AppleASAfirewall so that the users of Apple head office could access the DNS, HTTP, FTP and SMTP servers on the internet.
3. Configuration of static NAT on Apple ASA firewall so that users on the Internet could access the HTTP, FTP and SMTP servers in the DMZ network of Apple head office.
4. Configuration of access-lists considering the pre-nat and post-nat interfaces.

Chapter no 5: Configuration of the Juniper firewall of Lemon Head office with security policies and NAT

Concepts learnt and practised:

1. Configuration of security policies on Juniper firewall to allow different network traffic according to the specification
2. Configuration of source NAT on Lemon Juniper firewall so that the users of Lemon head office could access the DNS, HTTP, FTP and SMTP servers on the internet.
3. Configuration of static NAT on Lemon Juniper firewall so that users on the Internet could access the HTTP, FTP and SMTP servers in the DMZ network of Lemon head office.
4. Configuration of security policies considering the pre-nat and post-nat interfaces.
5. Configuration of Proxy-ARP on the juniper firewall

Chapter no 6: Configuration of the Paloalto firewall of Coconut head office with security policies and NAT

Concepts learnt and practised:

1. Configuration of security policies on Paloalto firewall to allow different network traffic according to the specification
2. Configuration of dynamic NAT on Lemon Juniper firewall so that the users of Lemon head office could access the DNS, HTTP, FTP and SMTP servers on the internet.
3. Configuration of static NAT on Lemon Juniper firewall so that users on the Internet could access the HTTP, FTP and SMTP servers in the DMZ network of Lemon head office.
4. Configuration of security policies considering the pre-nat and post-nat interfaces.

Chapter no 7: Configuration of the Checkpoint firewall of Mango head office with security policies and NAT

Concepts learnt and practised:

1. Configuration of the Gaia systems with IP address and static routes
2. Installation of Security Management Server, Security gateway and Smart console applications on the relevant systems
3. Configuration of security policies on Checkpoint firewall to allow different network traffic according to the specification
4. Configuration of Hide mode NAT on Mangocheckpoint firewall so that the users of Mango head office could access the DNS, HTTP, FTP and SMTP servers on the internet.
5. Configuration of static NAT on Mango checkpoint firewall so that users on the Internet could access the HTTP, FTP and SMTP servers in the DMZ network of Mango head office.
6. Configuration of NAT on Checkpoint firewall, using both Automatic and Manual configuration methods.
7. Configuration of security policies considering the pre-nat and post-nat interfaces.
8. Configuration of Static PAT

Chapter no 8: Understanding the basic concepts of Cryptography

Concepts learnt:

1. Importance of Security features like Confidentiality, Integrity, Accountability and Authentication for communication through Internet
2. Understanding the basics of cryptography like Key, algorithm, Public key, Private Key, Symmetric and Asymmetric encryption, digital signatures, digital certificates, Certificate Authority (CA), and Hash functions.
3. Understanding the role of IPSec protocols like Encapsulating Security Payload (ESP) and Authentication Header (AH) in securing TCP/IP communication
4. Understanding the role of Internet Key Exchange (IKE) in preparing the background for IPSec protocols
5. Capture and analysis of ISAKMP, ESP and AH protocol packets
6. Configuration of Certificate Authority and use of digital certificates for authentication

Chapter no 9: Configuration of the IOS firewall of Banana head office and branch offices with Point-to-Point GRE tunnels to enable site to site VPN

Concepts learnt and practised:

1. Understanding the concept and configuration of the Tunnel interfaces
2. Configuration of Site-to-Site VPN using GRE Point-to-Point tunnels

Chapter no 10: Configuration of the IOS firewall of Banana head office and branch offices with Point-to-Point GRE tunnels to enable site to site VPN

Concepts learnt and practised:

1. Understanding the concept and configuration of the Tunnel interfaces
2. Configuration of Site-to-Site VPN using GRE Point-to-Point tunnels

Chapter no 11: Configuration of the IOS firewall of Carrot head office and branch offices with Multipoint GRE tunnels to enable site to site VPN

Concepts learnt and practised:

1. Configuration of Site-to-Site VPN using GRE Multipoint tunnels
2. Understanding the concepts and configuration of NHRP protocol

Chapter no 12: Configuration of the IOS firewall of Pumpkin head office and branch offices with IPSec Site to site VPN

Concepts learnt and practised:

1. Understanding the concept and configuration of IKE
2. Understanding the concept and configuration of IPSec

3. Understanding the concept and configuration of crypto maps
4. Configuration of Site-to-Site IPSec VPN
5. Configuration of Route-maps to define interesting traffic for NAT
6. Understanding the configuration of security policies on IOS firewall using access-lists in combination with NAT and IPSec VPN

Chapter no 13: Configuration of the IOS firewall of Banana head office and branch offices with IPSec over GRE

Concepts learnt and practised:

1. Understanding the concept and configuration of IPSec profiles
2. Understanding the concept and configuration of protecting the GRE tunnels with IPSec profiles
3. Understanding the configuration of security policies on IOS firewall using access-lists in combination with NAT and IPSec over GRE

Chapter no 14: Configuration of the IOS firewall of Carrot head office and branch offices with IPSec over GRE

Concepts learnt and practised:

1. Understanding the concept and configuration of IPSec profiles
2. Understanding the concept and configuration of protecting the GRE tunnels with IPSec profiles
3. Understanding the configuration of security policies on IOS firewall using access-lists in combination with NAT and IPSec over GRE

Chapter no 15: Configuration of the ASA firewalls of Apple head office and branch offices with IPSec Site to site VPN

Concepts learnt and practised:

1. Configuration of Site-to-Site IPSec VPN on ASA firewalls
2. Understanding the configuration of security policies on ASA firewall using access-lists in combination with NAT and IPSec VPN

Chapter no 16: Configuration of the Juniper firewalls of Lemon head office and branch offices with IPSec Site to site VPN

Concepts learnt and practised:

1. Configuration of Site-to-Site IPSec VPN on Juniper firewalls
2. Understanding the configuration of security policies on Juniper firewall in combination with NAT and IPSec VPN

Chapter no 17: Configuration of the Paloalto firewalls of Coconut head office and branch offices with IPSec Site to site VPN

Concepts learnt and practised:

1. Configuration of Site-to-Site IPSec VPN on Paloalto firewalls
2. Understanding the configuration of security policies on Paloalto firewall in combination with NAT and IPSec VPN

Chapter no 18: Configuration of the Checkpoint firewalls of Orange head office and branch offices with Domain based IPSec Site to site VPN

Concepts learnt and practised:

1. Configuration of Domain based Site-to-Site IPSec VPN on Checkpoint firewalls
2. Understanding the configuration of security policies on Checkpoint firewall in combination with NAT and IPSec VPN

Chapter no 19: Configuration of the Checkpoint firewalls of Orange head office and branch offices with Route based IPSec Site to site VPN

Concepts learnt and practised:

1. Configuration of VPN tunnel interfaces on Checkpoint firewalls
2. Configuration of route based Site-to-Site IPSec VPN on Checkpoint firewalls

Chapter no 20: Configuration of the Orange Checkpoint deployment to install security policies on the head office and branch office firewalls without Control connections implied rules

Concepts learnt and practised:

1. Understanding the importance of Checkpoint services like CPD (18191), CPD_Amon(18192), FW1(256), FW1_Log(257), FW1_ICA Push(18211)

Chapter no 21: Configuration of the Orange Checkpoint deployment to install security policies on the head office and branch office firewalls with Control connections implied rules

Concepts learnt and practised:

1. Understanding the importance of Checkpoint services like CPD (18191), CPD_Amon(18192), FW1(256), FW1_Log(257), FW1_ICA Push(18211)
2. Installation of security policies on branch office firewalls using centralized Security Mangement Server

Chapter no 22: Configuration of the Tomato Checkpoint deployment with User and Client authentication

Concepts learnt and practised:

1. User and Client authentication
2. Active Directory concepts and Integration of Checkpoint with Active directory

3. Concepts and configuration of Identity Awareness including AD query, Captive Portal (Browser based authentication) and Identity agent

Chapter no 23: Configuration of the Tomato Checkpoint deployment with IPSec Remote Access VPN

Concepts learnt and practised:

1. Office mode, Hub mode, and Visitor mode
2. Policy server and Desktop policies

Chapter no 24: Configuration of the Tomato Checkpoint deployment with SSL VPN

Concepts learnt and practised:

1. Configuration of SSL VPN on Checkpoint

Chapter no 24: Configuration of the Coconut Paloalto deployment with Remote access VPN

Concepts learnt and practised:

1. Configuration of remote access VPN on Paloalto firewall

Chapter no 25: Configuration of the Cucumber Checkpoint deployment with Cluster XL cluster

Concepts learnt and practised:

1. Configuration of clustering of the Checkpoint firewalls with Cluster XL

Chapter no 26: Configuration of the Ginger Checkpoint deployment with VRRP cluster

Concepts learnt and practised:

1. Configuration of clustering of the Checkpoint firewalls with VRRP

Chapter no 27: Configuration of the Potato, Brinjal and Cabbage Checkpoint deployment with virtualization

Concepts learnt and practised:

1. Configuration of Virtual system extension gateway
2. Configuration of Virtual systems
3. Configuration of Virtual routers
4. Configuration of Virtual switches
5. Configuration of advanced routing