NETWORK SECURITY WITH FIREWALL

Course Objectives

To demonstrate the features of firewall in providing network security for an enterprise with a real time case study comprising of 200+ systems, 50+ routers and 20+ firewalls.

All the configuration and troubleshooting tasks that are mentioned below are demonstrated live in the workshop explaining the concepts. Only the IP addresses would have been pre assigned to the routers and the systems.

Case study description

The case study is divided into 9 autonomous systems managed by 9 different service providers simulating Internet environment. Different organizations listed below are connected to the Internet with different network resources like HTTP, FTP, POP3 and SMTP servers.

Real time simulated Case study with network of over 15 organizations, Yahoo, Gmail and Go-Mummy having their HTTP, FTP, POP3 and SMTP servers on public network some Internet client systems

Routing in the Case study

Dynamic routing is done within the autonomous systems by using routing protocols like RIP, OSPF and EIGRP. Routing in between the autonomous systems is done by BGP routing protocol. Static routes and default routes are also configured in the case study. Redistribution between the routing protocols is also done so that the systems with public IP addresses are reachable by each other.

Configuration of the ISP-DNS server

- Configuration of zones, domains and host records on the ISP-DNS server for various organizations in the case study
- Configuration of MX records on the ISP-DNS server so that various Mail servers in the case study could find the IP addresses of each other while relaying the mail to different organizations.

Installation of the various Checkpoint applications and deployment of security policies

- Installation of Gaia OS
- Configuration of the interfaces and static routing
- Installation of Primary management sever
- Installation of Secondary management server
- Installation of Log server
- Installation of Smart console
- Integration of all the Checkpoint components by enabling SIC
- Deployment of security policies
- Analysing the logs using Smart View Tracker
- Configuration of Management high availability
- Resetting of SIC
- Configuration of different administrators with different permission profiles
- Configuration of additional GUI clients

Network Address Translation

Understanding the configuration of NAT so that the servers on the Internet with public IP addresses are reachable for various services like HTTP, FTP, DNS, SMTP etc by systems in the private networks

Understanding the configuration of NAT so that the servers on the DMZ networks with private IP addresses are reachable for various services like HTTP, FTP, DNS, SMTP etc by systems on the Internet.

- Configuration of Hide mode NAT and Static NAT
- Configuration of automatic NAT rules
- Configuration of manual NAT rules
- Configuration of Static PAT
- NAT and Proxy ARP
- NAT and security policy rules

Checkpoint Services

- Understanding the Checkpoint services like CPD, CPD Amon, fw1, Fw1_log, ICA push certificate etc
- Understanding the Checkpoint control connections
- Configuration of the branch office firewallswith security policy without control connection implied rules
- Configuration of the branch office firewalls with security policy with control connection implied rules

Authentication and Authorization

Understanding the configuration of security rules so that only certain authorized usersaccess the intended resources on the Internet

- Configuration of User authentication
- Configuration of Session authentication
- Configuration of manual Client authentication
- Configuration of partially automatic Client authentication
- Configuration of fully automatic Client authentication
- Integration of firewall with Active directory
- Configuration of LDAP account units and LDAP groups
- Configuration of Identity Awareness
- Configuration of AD query
- Configuration of Captive Portal or Browser based authentication
- Configuration of Identity agents

Content Security

Understanding the configuration of resources to provide content security for various services

- Configuration of content security for FTP by creating an FTP resource
- Configuration of content security for SMTP by creating an SMTP resource
- Integration of checkpoint with a third party CVP server for Virus checking

Understanding the installation of an external CA in the case study

Configuration of security rules so that the users could access their mail server in the DMZ from the Internet using the following protocols

- HTTP
- HTTPS
- POP3
- IMAP
- POP3 over SSL
- IMAP over SSL

Virtual Private Networks

Understanding the configuration of IPSEC VPNs so that the communication between the systems in the head office, branch offices, remote users and business partner's networks secured with encryption.

- Configuration of domain based site-to-site VPN in meshed topology
- Configuration of domain based site-to-site VPN in Star topology without VPN routing
- Configuration of domain based site-to-site VPN in Star topology with VPN routing
- Configuration of domain based site-to-site VPN between the business partners with authentication by a shared secret
- Configuration of domain based site-to-site VPN between the business partners with authentication by digital certificates. Configuration of trust between the external CAs
- Configuration of Route based VPN between the head office and the branch offices with static routing
- Configuration of Route based VPN between the head office and the branch offices with dynamic routing by configuring OSPF on the firewalls
- Configuration of Route based VPN between the head office and the branch offices with dynamic routing by configuring BGP on the firewalls
- Configuration of Site-to-client VPN with Secure Remote client
- Configuration of Site-to-client VPN with Secure client
- Configuration of desktop policies for the Secure client
- Configuration of office mode for the Secure client with the firewall issuing an IP from the IP pool
- Configuration of office mode for the Secure client with the firewall issuing an IP from the DHCP server acting as a DHCP Relay agent
- Configuration of reservation of IP addresses for the remote users in office mode
- Configuration of Hub mode for remote users
- Configuration of Visitor mode for the remote users

Deployment of firewalls in a cluster

- Configuration of a cluster of firewalls with Cluster XL
- Configuration of a cluster of firewalls with VRRP
- Configuration of Load balancing and High availability clusters

Virtualization

- Configuration of Virtual gateway
- Configuration of Virtual systems
- Configuration of Virtual routers
- Configuration of Virtual switches
- Configuration of advanced source based routes
- Deployment of security policies

Deployment of security policies in a NOC environment

- Installation of Multi domain security server
- Deployment of security policies using Multi domain security server