IT412- SYSTEM ADMINISTRATION & MAINTENANCE

SECURITY AND ACCESS CONTROLS

Topics:

01 Access Control List

02 Firewall Setup and Configuration

03 Intrusion Detection and Prevention System

04 Authentication and Authorization

1. ACCESS CONTROL LIST

ACL (Access Control List) - is a set of rules used to control network traffic and reduce network attacks. It defines which incoming or outgoing packets are allowed or denied based on factors like IP addresses, protocols, and ports.

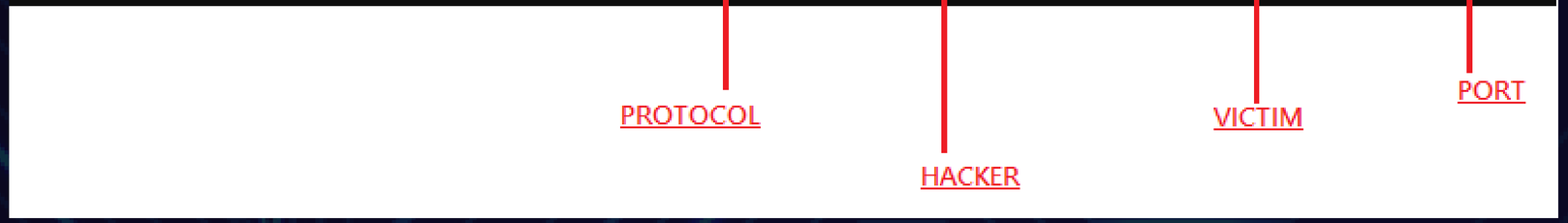
Types of Network ACL

- **Standard ACL**
- **Extended ACL**

CONT..

Extended ACL

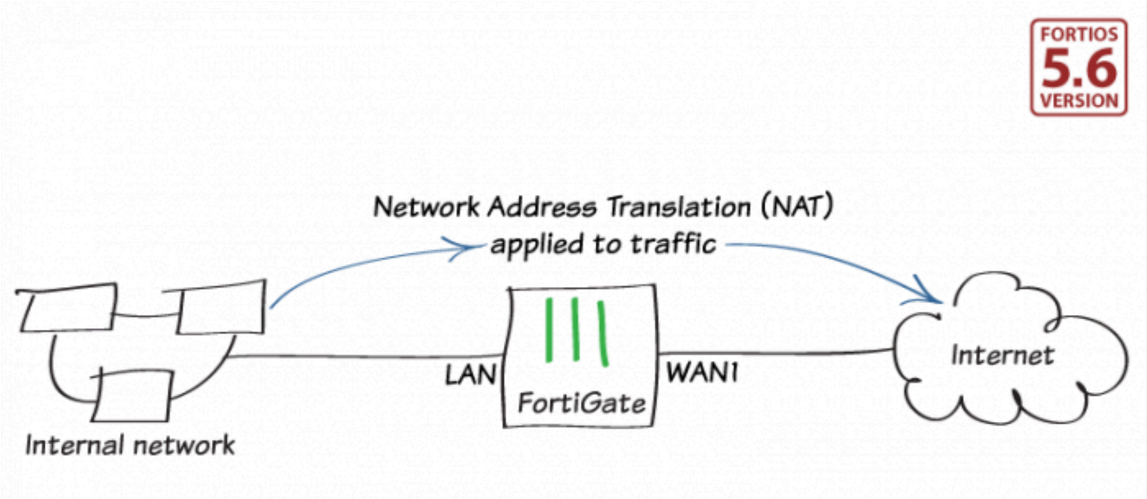
```
Router(config)# access-list 101 deny tcp host 192.168.1.2 host 192.168.1.1 eq 19
Router(config)# access-list 101 deny udp host 192.168.1.2 host 192.168.1.1 eq 19
```

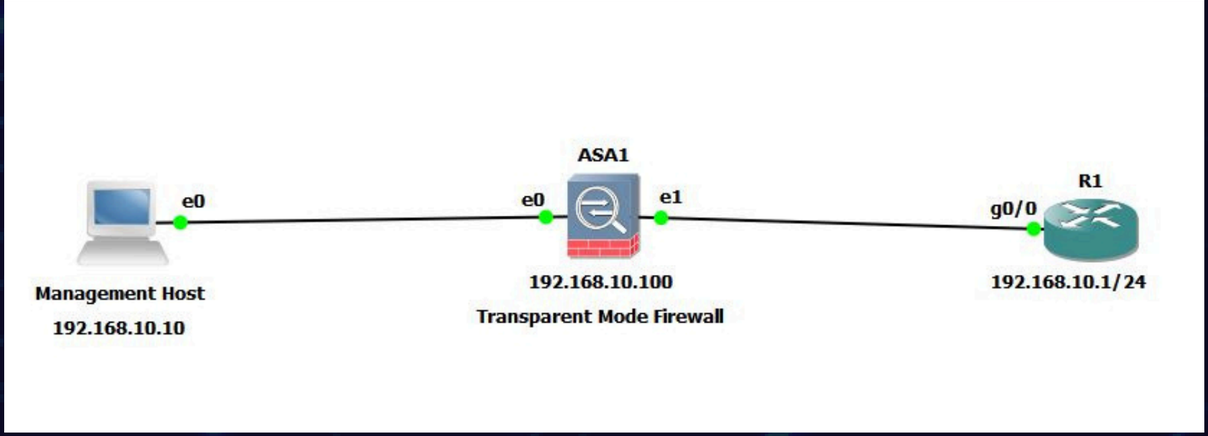


2. FIREWALL SETUP

01 NAT Mode or Route Mode

02 Transparent Mode or Bridge Mode





3. INTRUSION DETECTION AND PREVENTION SYSTEM

An intrusion detection and prevention system (IDPS) is a solution that monitors a network for threats and then takes action to stop any threats that are detected.

ZERO DAY ATTACK?

A zero-day is a vulnerability in software or hardware that is typically unknown to the vendor and for which no patch or other fix is available. The vendor has zero days to prepare a patch as the vulnerability has already been described or exploited

CONT..


Antivirus
Intrusion Prevention
Indicators of Compromise
IoC
Mobile Security
Web Security
Threat Intelligence Service
Security Rating Service
Antispam
FortiGuard Services
Web Filtering
Vulnerability Management
Application Control
Virus Outbreak Protection Service
Cloud Access Security Broker
Industrial Security
Content Disarm & Reconstruction
IP Reputation

4. AUTHENTICATION AND AUTHORIZATION

Authentication - the process of verifying user identity before giving them permission to access a system, account, or file.

Authorization - the process of verifying a user's access level to a system, account, or file.

THANK YOU