Network security 1

Week 1

Introduction

Content

- Concepts of network security
- Security configuration of network devices
- AAA
- Firewall
- IPS and IDS
- Introduction to VPN
- Security configuration for LAN

Goals

- Configure network devices for secure communication
- Apply the knowledge to deploy different types of VPN for secure communicatoon over unreliable networks based on different standards
- Design and implemente different types of firewall based on network requirements

Chapter 2

Securing the edge router

An edge router is a router which connect a network to the internet.

The Single Router Approach has a single edge router between a network and the internet. A Defense in Depth Approach has a router connection to the internet, a firewall and then another router connected to the LAN. A DMZ (de militarized zone) Approach is similar, but the firewall is a DMZ.

Three areas of router security

1. Physical security
    1. A lock
    2. Smoke alarms
    3. UPS
    4. Humidity etc.
2. Router OS config file security
    1. Backup copy
    2. Secure configuration
3. Router hardening

1. Disable telnet
2. Closing unused ports

Secure Administrative Access

- Restrict device accessibility (`line console`)
- Log and account for all access (`enable secret`)
- Authenticate access
- Autorize actions
- Present legal notifaction (`banner motd`)
- Ensure the confidentiality of data (limit copy of config file etc.)

A PC with a terminal emulator is required, prefably over SSH or HTTPS (not telnet or http). Security is always a trade-off.

Configuring a secure router

Increasing access security

The algorithm md5 is type 5, scrypt 9 and sha256 8.

```
security passwords min-length 10
service password-encryption
lne vty 0 4
exec-timeout 3 30
line console 0
exec-timeout 3 30
enable algorithm-type [md5 | scrypt | sha256] secret [password]
username [name] algorithm-type [md5 | scrypt | sha256] secret [password]
```

```
banner [motd | exec | login] [delimiter] [message] [delimiter]
```

```
login block-for [seconds] attempts [tries] within [seconds]
# Create an access list and add the admin
login quiet-mode access-class [acl-name|acl-number]
login delay [seconds]
login on-success log [every [login]]
login on-failure log [every [login]]
```

```
ip access-list standard PERMIT-ADMIN
remark Permit only Administrative..
# complete (page 9 chapter)
```

```
line console 0
# Login with local username and passwords (not some for all)
login local
end
exit

username user01 algorithm-type scrypt secret user01pass
```

Configuring privilege levels

Level 0-15:

0: Predefined for user-level access privileges

15: reserved for the enable mode privileges (admin / highest)

```
privilege mode (level level | reset) command

privilege exec level 5 ping
enable algorithm-type scrypt seret level 5 cisco5
username SUPPORT privilege 5 algorithm-type scrypt
```

A better way is to create views (administrative roles).

Views (administrative roles)

We have three views; root view (similar to privilege 15). Superviews consist of views. View contain commands. Superview users can use the commands available in the views of the superview.

```
# create a root view (highest privilege)
# enable view

# Create a view
parser view admin1
secret admin1pass
# Check available commands
commands ?
# Add some allowed commands
commands exec include all show
commands exec include all config terminal
commands exec include all debug
end

# Use the view
enable view admin1
# Verify available commands
?
```

```
# create a superview
parser view mysuperview superview
secret superviewpass
# add views to the superview
view myview
```

Highest admin:

- `commands exec include all show`
- `commands exec inclue all config terminal`
- `commands exec include all debug`

Second highest admin (junior):

- `commands exec include all show`

Tech (installs end-user devices and cabling):

- `commands exec include show version`
- `commands exec include show interfaces`
- `commands exec include show ip interface brief`
- `commands exec include show parser view`

Secure copy (SCP)

Uses SSH

1. Configure SSH
2. Configure one user with privilege 15
3. Enable AAA
4. Specify the local database for authentication
5. Configure command authorization
6. Enable SCP

```
security authentication failure rate [rate] log
show login failures
```

Always enfore the latest version (SSH version 2). When creating the username, add `algorithm-type scrypt` .

```
ip ssh time-out 60
ip ssh authentication-retries 2
```

Use SSH as the default way to connect / administrate.

```
line vty 0 4
privilege level 15
login local
transport input ssh
```

```
exit

crypto key zeroize rsa

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

ip ssh time-out 90
ip ssh authentication-retries 2

username admin privilege 15 algorithm-type scrypt secret cisco12345

# enable scp server (secure copy)
ip scp server enable
```

```
# Show currently logged in users
show users
```

```
##config aaa
# Enable aaa
aaa new-model
# use local database
aaa authentication login default local
# use local database
aaa authorization exec default local

# enable root view
enable view
# create a view
parser view admin1
#set password
secret admin1pass
# view commands
commands ?
# delete a view
no parser view admin1
```

```
# send files between routers
R1# copy running-config R1-Config
R1# show flash

R3# copy scp: flash:
```

Type of management

In bound:

- Apply only to devices needed to be managed or monitored
- Use SSH or SSL
- Decide if it needs to be opened at all times

Out of bounds:

- Highest level of security
- Mitigate the risk of management over the network

Syslog

Start TFPD64 on a PC connected to the network.

```
service timestamps log datetime msec
logging host 192.168.1.3
# Find a severity level
logging trap ?
# Select a severity level
logging trap [level]
show logging
```

```
# Format
sequintal number:timestamp:source / cause:severity:message:description
```

Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unstable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

SNMP

Simple Network Management Protocol. We use SNMPv3 (Management Information Base - MIB). We use SNMPv3 level authPriv (authentication via HMAC-MD5 or HMAC-SHA and encryption via DES, 3DES or AES).

SNMP is vulnerable. If other methods are available - use them. Always use authentication, encryption and a ACL (to control from what sources messages can come).

SNMP-RO means SNMP Read Only.

```
# configure a SNMP view called SNMP-RO to include the ISO MIB family
snmp-server view SNMP-RO iso included
# Create a group, SNMP-G1 which requires both authentication and encryption - restrict SNMP access to local LAN
snmp-server group SNMP-G1 v3 priv read SNMP-RO access PERMIT-SNMP
# Configure a user SNMP-Admin to group SNMP-G1. Authention with Authpass and encryption with Encrypass
snmp-server user SNMP-Admin SNMP-G1 v3 auth sha Authpass priv aes 128 Encrypass
# Verify
show snmp group
show snmp user

```

```
# Example
ip access-list standard PERMIT-ADMIN
permit 192.168.1.0 0.0.0.2555
exit
snmp-server view SNMP-RO iso included
snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
...
```

chapter 2 (page 66-ish)

SNMP agent sends an SNMP trap to SNMP server.

NTP

Network Time Protocol. Time synchronization is important.

```
R2# show clock
R2# clock set 14:54:20 Sep 4 2018
R2(config)# ntp authentication-key 1 md5 NTPpassword
R2(config)# ntp trusted-key 1
R2(config)# ntp authenticate
R2(config)# ntp master 3

R1(config)# ntp authentication-key 1 md5 NTPpassword
# A server without the trusted-key cannot change the time
R1(config)# ntp trusted-key 1
R1(config)# ntp authenticate
R1(config)# ntp server 10.1.1.2
R1(config)# ntp update-calendar

R1# show ntp associations
R1# debug ntp all
R1# undebug all
```

```
R1# show clock
```

Permorming a security audit

CDP - Cisco Discovery Protocol can retrieve informtion about neighbors.

LLDP - link layer discovery protocol works on all devices regardless of vendor (open source).

```
lldp run

show cdp neighbors detail
show lldp neighbors detail
```

The protocols should be turned off in a production network.

We usually also want to:

- disable uneccessary services
- ...

page 63 chapter 2

OSPF (routing authentication)

We need to be able to trust routing update. Authentication prevents spoofing.

```
# Do this procedure for all routers!

# Assign key chain name and number
key chain NetAcad
key 1
# Assign authentication key
key-string CCNASkeystring
cryptographic-algorithm hmac-sha-256

# For all used serial interfaces
interface s0/0/0
ip ospf authentication key-chain NetAcad

show ip ospf interface s0/0/0
show ip ospf neighbor
show ip ospf route
```

Week 2

Chapter 3

AAA

AAA - Authentication Authroization and Accounting

Authentication: Who are you? Authorization: What can you do? Accounting: What did you do?

Accounting creates a start message for an authorized user and later a stop message. Accounting includes network, connection, EXEC, system, command, resource.

Local AAA authentication:

1. Client establishes connection with router
2. AAA router prompts user for username password
3. Router authenticates the user

Enable local AAA authentication on all logins with case-sensitivity:

```
username JR-ADMIN algorithm-type scrypt secret SuchP4ssw00rd
username ADMIn algorithm-type scrypt secret MuchW0w0
aaa new-model
--- Alt 1
aaa authnetication login default local-case
--- Alt 2
aaa authentication login default local-case enable
aaa authentication login SSH-LOGIN local case
line vty 0 4
login authentication SSH-LOGIN
```

Remote AAA authentication:

Used for larger networks.

1. Client establishes connection with router
2. AAA router prompts user for username password
3. Router authenticates with a remote AAA server
4. The user get authorized

Uses TACACS+ (CISCO) or RADIUS (Open Source, widely used) as a protocol. RADIUS uses UDP, has extensive accounting etc. TACACS+ uses TCP, has limited accounting etc.

```
# Configure TACACS+
aaa new-model
tacacs server Server-T
address ipv4 192.168.1.101
single-connection
key TACACS-pAssword
```

```
# Configure RADIUS
aaa new-model
radius server SERVER-R
# Set auth port and accounting port (same as for server)
address ipv4 192.168.1.100 auth-port 1812 acct-port 1813
key RADIUS-password
```

```
# Enable authentication via TACACS+ and RADIUS
aaa authentication login default group tacacs+ group radius local-case
# Debug
debug radius ?
debug tacacs ?
```

Locking users

```
# Lock users after failed attempts
aaa local authentication attempts max-fail [number]
# Show locked out users
show aaa local user lockout
# Show aaa sessions
show aaa sessions

# Show debugging options
debug aaa ?
```

802.1X (dot1x)

Used for network access control.

```
# On a switch
aaa new-model
radius server CCNAS
address ipv4 192.168.1.100 auth-port 1812 acct-port 1813
key RADIUS-APSSWORD
aaa authentication dot1x default group radius
dot1x system-auth-control
interface F0/1
description Access Port
switchport mode access
authentication port-control auto
dot1x pae authentication
```

Week 3

Implementing firewall

```
# Create three zones
zone security INSIDE
zone security CONFROOM
zone security INTERNET

# Configure a inspect class-map to match traffic allowed from INSIDE
zonte to INTERNET
class-map type inspect match-any INSIDE_PROTOCOLS
```

```
match protocol tcp
match protocol udp
match protocol icmp

class-map type inspect match-any CONFROOM_PROTOCOLS
match protocol http
match protocol https
match protocol dns

# Enable policy maps
policy-map type inspect INSIDE_TO_INTERNET
class type inspect INSIDE_PROTOCOLS
inspect

policy-map type instpect CONFROOM_TO_INTERNET
class type inspect CONFROOM_PROTOCOLS
inspect

zone-pair security INSIDE_TO_INTERNET source INSIDE destination INTERNET
zone-pair security CONFROOM_TO_INTERNET source CONFROOM destination INTERNET

zone-pair security INSIDE_TO_INTERNET
service-policy type inspect INSIDE_TO_INTERNET

zone-pair security CONFROOM_TO_INTERNET
service-policy type inspect CONFROOM_TO_INTERNET

show zone-pair security
show policy-map type inspect zone-pair
show zone security
```

Access Control List

The basic firewall - basic defence. Used in all systems. See notes part 1 and 2.

An ACL can be applied to interfaces and virtual lines (VTY - telnet, ssh).

ACLs are used to filter traffic. They can also be used to mitigate some attacks such as DoS and spoofing.

Mitigate ICMP abuse

```
# Mitigate ICMP abuse (S0/0/0 to internet)
access-list 112 permit icmp any any echo-reply
access-list 112 permit icmp any any source-quench
access-list 112 permit icmp any any unreachable
access-list 112 deny icmp any any
access-list 112 permit ip any any
```

```
# Mitigate ICMP abuse (G0/0 inside to user)
access-list 112 permit icmp 192.168.1.0 0.0.0.255 any echo
access-list 112 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem
access-list 112 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big
access-list 112 permit icmp 192.168.1.0 0.0.0.255 any source-quench
access-list 112 deny icmp any any
access-list 112 permit ip any any
```

Mitigate SNMP exploits

```
# Prefable
no snmp-server
# Tolerable
# only allow from administrative snmp host address
```

IPv6

An IPv4 ACL does not consider IPv6.

ACL syntax...

Week 3

IPS and IDS

IDS (Intrusion Detection System)

- Works passively
- Requires traffic to be mirrored in order to reach it
- Networktraffic does not pass through the IDS unless it is mirrored

IPS (Intrusion Prevention System)

- Implemented in an inline mode
- Monitors Layer 3 and Layer 4 traffic
- Can stop single packet attacks from reaching target
- Responds immediately, not allowing any malicious traffic to pass
- Introduces delay - inspects each packet

- Both technologies are deployed as sensors

- Both technologies use signatures to detect patterns of misuse in network traffic
- Both can detect atomic patterns (single-packet) or composite patterns (multi-packet)
- Some say IDS is preffered, some say IPS. We say they are complementary - use both!

Advantages

IDS

- No impact on network
- No network impact if there is a sensor failure
- No network impact if there is a sensor overload

IPS

- Stops trigger packets
- Can use stream normalization techniques

Disadvantages

IDS

- Response action cannot stop trigger
- Correct tuning required for response actions
- More vulnerable to network security evasion techniques

IPS

- Sensor issues might affect network traffic
- ...

Host-Based vs Network-Based

Advantages

Host-Based

- Provides protection specific to a host OS
- Provides OS and application level protection
- Protects the host after the message is decrypted
- Does not work with encrypted messages

Network-Based

- Cost effective
- OS independent
- Not visible to the network
- Lower level network events seen

Disadvantages

Host-Based

- OS dependent
- Must be installed on all hosts

Network-Based

- Cannot examine encrypted traffic
- Cannot determine whether an attack was successful
- Must stop malicious traffic prior to arriving at host

Port Mirroring (SPAN)

A hub broadcasts network packets - no port mirroring needed. Switches populate a MAC table, therefore we need to enable port mirroring (traffic sniffing).

CISCO calls it SPAN.

```
Switch(config)# monitor session [number] source [interface interface | vlan vlan]
Switch(config)# monitor session [number] destination [interface interface | vlan vlan]
Switch# show monitor
```

Signature Alarm

- Pattern-based detection
- Anomaly-based detection
- Policy-based detection
- Honey pot-based detection

IPS signature attributes

- Type
  - Atomic
  - Composite
- Action
  - Generate an alert
  - Log the activity
  - Drop or prevent the activity
  - Reset a TCP connection
  - Block future activity
  - Allow the activity
- Trigger (alarm)
  - Pattern-based detection
  - Anomaly-based detection
  - Policy-based detection
  - Honey pot-based detection

Patter-based detection

- Known as signature-based detection
- Simplest triggering mechanism

- Search for specific and pre-defined pattern
- Compares the network traffic to a database of known attacks, and triggers an alarm or prevents communication if a match is found
- Only works for known attacks

Anomaly-based detection

- Known as profile-based detection
- The administrator defines a profile for normal activity by monitoring activity on the network or host over a period of time
- New and previously unpublished attacks can be detected
- An alert from an anomaly signature does not necessarily indicate an attack
- Administrator must guarantee that the network is free of attack traffic during the learning phase
- If the attack traffic happens to be similar to normal traffic, the attack might go undetected

Policy-based detction

- Known as behavior-based detection
- The administrator defines behaviors that are suspicious based on historical analysis
- Enables a single signature to cover an entire class of activites without having to specify each individual situation

Honey pot-based detection

- Use a dummy server to attract attacks
- The purpose of the honey pot approach is to distract attacks away from real network devices
- Security vendors tend to use them for research

Implement IOS IPS

1. Download the IOS IPS
2. Create IOS IPS config directory in Flash
3. Configure an IOS IPS crypto key
4. Enable IOS IPS
5. Load the IOS IPS signature package to the router

```
# Create folder
mkdir ips-configs
# Rename folder
rename ips-configs ips-config
# List directories in Flash
dir

# Copy content of key to IOS CLI
# Check if it is available
show run

```

```
# Enable
ip ips name IOSIPS
ip ips name IOSIPS ?
ip ips config location flash:<directory-name>
ip ips notifiy [sdea | log]
ip ips signature-category
category all
# Don't compile signatures
retired true
exit
category ios_ips ?
category ios_ips basic
# Compile signatures
retired false
end

interface G0/0
ip ips IOSIPS in
exit
interface G0/1
ip ips IOSIPS in
ip ips IOSIPS out
end

copy tftpd://192.168.1.3/IOS-S41....pkg idconf

show ip ips signature count
```

```
show ip ips
show ip ips all
show ip ips configuration
show ip ips interfaces
show ip ips signatures
show ip ips statistics

# Disable IPS
clear ip ips configuration
clear ip ips statistics
```

Attacks

attacks and layer...

Week 4

DHCP spoofing

1. PC (DHCP DISCOVER - broadcast): I would like to request an address

2. DHCP (DHCP OFFER - unicast): I am server 1. Here is an address
3. PC (DHCP REQUEST - broadcast): I accept the address
4. DHCP (DHCP PACK - unicast): I acknowledge your request

DHCP Starvation attack

The attacker sends DHCP DISCOVER for each address available in netmask. Then the attacker accepts each address, which the server acknowledges. Then the server won't have any addresses left. Mitigate with port security. Limit by MAC address and port.

DHCP Snooping

We can configure trusted and untrusted ports. Ports facing clients can be untrusted - within the network it can be trusted.

```
# Allow dhcp on router port
ip dhcp snooping
interface F0/1
ip dhcp snooping trust
exit

# Limit dhcp on switch ports
interface range F0/5-24
ip dhcp snooping limit rate 6
exit

# Activate snooping on vlan
ip dhcp snooping vlan 5,10,50-52

# Verify config, learn options
show ip dhcp snooping
show ip dhcp snooping binding
```

ARP Spoofing

Any device getting an ARP request can respond with their MAC address. To mitigate we need to enable DHCP spoofing. It basically works the same way, tracking trusted and untrusted ports.

```
ip dhcp snooping
ip dhcp snooping vlan 10
ip arp inspection vlan 10

interface Fa0/24
ip dhcp snooping trust
ip arp inspection trust

# Show available inspection modes
ip arp inspection validate ?
```

VPN

Benefits: cost savings, security (if those features are used), scalability, compatibility (OS, routers, devices).

Usually we think of two possible types; Remote-Access VPN (end user to site) and Site-to-Site VPN access (end uses don't care about VPN connection - gateways take care of it via encapsulation). A VPN does not guarantee security, we use a second protocol for this.

IPsec

Framework

It's a standard implementation. It's used to protect and authenticate IP packets between source and destination. Protect virtually all traffic from layer 4 through 7 (it rests in layer 3). Confidentiality using encryption, integrity using hashing, authentication using Internet Key Exchange and secure key exchange using Diffie-Hellman. It's not bound to a specific algorithm, it's rather a framework - flexible.

Usually we use HMAC (SHA-2) for integrity. Confidentiality is gained through AES or SEAL (note: seal is patented and not well studied). Authentication is carried out using Pre-Shared Key (PSK) or a Public Key Infrastructure (PKI). PSK use hash algorithms (PBKDF2 etc.), PKI use RSA. Secure Key Exchange (SKE) use Diffie-Hellman (DH). For DH use versions equal to or larger than 19 (21 is 4096 bit RSA, 24 is elliptic curves). Do not ever use 14-15! The larger the better.

To summarize; the *framework* for IPsec is:

- Confidentiality
- Integrity
- Authentication
- Secure Key Exchange

Protocol

We could encrypt everything except for the most important header values (IP, TTL etc.). Another option is to use encapsulation techniques.

Authentication Header (AH) does not provide confidentiality. The header is plain-text. The header is hashed for integrity. Data payload is encrypted.

ESP does provide encryption of the entire packet - it wraps the original packet in a new packet. There are two modes; Transport mode where Data and ESP Trailer is encrypted. Tunnel Mode where the IP Header is also encrypted (more secure).

Internet Key Exchange (IKE)

IKE is a key management protocol. Used for security negotation (IPsec protocol, confidentiality protocol, integrity protocol etc.).

Phase 1 - Negotatiate ISAKMP policy

1. ISAKMP policy is the security association (how they will create the tunnel).
2. DH key exchange

3. Verify peer identity

Phase 2 - Negotiate IPsec policy (what traffic should go through the tunnel etc.).

Configuring Site-to-Site IPSec VPN

We create two tunnels. First tunnel is ISAKMP, second tunnel - IPsec - is inside of that tunnel.

```
# Configure interesting traffic ACL
access-list [acl] permit udp source [wildcard] [destination] [wildcard] eq isakmp
access-list [acl] permit esp [source] [wildcard] [destination] [wildcard]
access-list [acl] permit ahp [source] [wildcard] [destination] [wildcard]
# Example - configure both sites!
R1(config)# access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 10.0.1.0 0.0.0.255

## Configure ISAKMP policy for IKE Phase 1
#

# Show defaults - sorted by descending security (not secure, though!)
show crypto isakmp default policy
crypto isakmp policy ?
# Configure policy
crypto isakmp policy 1
# Configure HAGLE - hash, authentication, group, lifetime, encryption
# Put ? after each command to see available
hash sha
authentication pre-share
group 24
lifetme 3600
encryption aes 256

show crypto isakmp policy

# Configure pre-shared key if we used that option
crypto isakmp key [keystring] address [peer-address]
crypto isakmp key [keystring] hostname [peer-hostname]

## Configure IPsec policy for IKE Phase 2
#

# Show configured security associations
show crypto isakmp sa

```

```
# Create a transform set (name is usually R1-R2 etc.) - on both routers!
crypto ipsec transform-set [name] [authentication] [encryption / integrity]

## Configure crypto map for IPsec policy
#

# If using key exchange, use isakmp, if not use ipsec-manual.
crypto map [map-name] [sequence-number] [ipsec-isakmp | ipsec-manual]
# Example
crypto map R1-R2_MAP 10 ipsec-isakmp
match address 101
set transform-set R1-R2
# R1 sets address to R2, R2 sets address to R1
set peer 172.30.2.2
# Set diffie-hellman group
set pfs group24
set security-association lifetime seconds 900

show crypto map

# Apply the IPsec policy

interface serial0/0/0
crypto map R1-R2_MAP

show crypto map

# Verify the IPsec tunnel is operational - the first packet will drop since the tunnel is not open yet
ping 192.168.1.1 source 10.0.1.1
# Show the active isakmp tunnels
show crypto isakmp sa
# Show active ipsec tunnels
show crypto ipsec sa
```

Week 5

Cisco Adaptive Security Appliance (ASA)

ASA provides Firewall, VPNs, IPSec etc. It has all security related functionality. It is commonly used as an edge device. There are different models (Small office / home office, medium, large etc.).

ASA can have different features all in one device. These features are called security context. NAT, VPN etc. will all work in isolation no matter the other configurations (virtualization).

ASA provides high availability. You can use the device for redundancy - config two devices with the exact same config. If the primary (active) device does not respond, the secondary will become active and keep the network up.

ASA supports Microsoft Active Directory (AD) and AD Agent - this can be used as an authentication server.

ASA will by default work with security levels (outside will become 0, inside will become 100). Lower levels cannot communicate with higher levels. By default outside won't be able to communicate with inside. Usually outside is 0, inside 100 and DMZ 50. The levels are used for Network Access, Inspection Engines and Application Filtering control.

The ASA device can work in either Transparent Mode (Layer 2 / switch mode - create VLANs, up to 5) and Routed Mode.

`show version` shows license information.

Command differences

```
ip route -> route outside
show ip interfaces brief -> show interfaces ip brief
? -> help
show vlan -> show switch vlan
copy running-config startup-config -> write [memory]
erase startup-config -> write erase
```

You do not need to write `do` before commands in global configuration mode to execute `show` commands.

Basic configuration ("old device" - 5505)

```
hostname CCNAS-ASA
domain-name ccnassecurity.com
enable password class
banner motd ...


# Configure password encryption
show password encryption
key config-key password-encryption cisco123
password encryption aes

show password encryption
# Store running configuration
write

# Create vlan
interface vlan [vlan-number]
nameif [inside | outside | dmz]
# Set optional security level (nameif sets it for us)
```

```
security-level [value]

# Configure IP addresses
# Static
ip address ip-address netmask
# DHCP
ip address dhcp
# DHCP and set default route upstream
ip address dhcp setroute

# Upstream DLS
ip address ppoe
# DLS and default route upstream
ip address ppoe setroute

# Static route
route outside 0.0.0.0 0.0.0.0 209.165.200.225
show route | begin Gateway

# Remote access (telnet)
# Accept from host 192.168.1.3 (from inside interface, mask means connected locally)
telnet 192.168.1.3 255.255.255.255 inside
telnet timeout
show run telnet

# Remote access (SSH)
username ADMIN password CISCO
aaa authentication ssh console LOCAL
crypto key generate rsa modulus 2048
# Accept from host 192.168.1.3 (from inside interface, mask means connected locally)
ssh 192.168.1.3 255.255.255.255 inside
ssh version 2
show ssh

# NTP authentication
ntp authenticate
ntp trusted-key 1
ntp authentication-key 1 md5 cisco123
ntp server 192.168.1.254

# DHCP server
# Limited to 43 addresses
dhcpd address 192.168.1.10-192.168.1.41 inside
dhcp lease 1800
```

Object and Object Groups

When configuring an object, only the last statement is used. To use multiple statements - create a group.

```
object ?
object-group ?
service ?

object network EXAMPLE-1
# Add a single host
host 192.168.1.3
# Add a range of hosts
range 192.168.1.10 192.168.1.20

show running-config object

object service EXAMPLE-2
serivce tcp destination eq ftp
service tcp destination eq www

show running-config object service
```

Groups:

- Network
- Service
- Security
- ICMP-type
- User

```
object-group network ADMIN-HOST
description Administrative hosts
network-object host 192.168.1.3
network-object host 192.168.1.4

object-group SERVICES-1
service-object tcp destination eq www
service-object tcp destination eq https
service-object tcp destination eq pop3
service-object tcp destination eq ntp

object-group service SERVICES-2 tcp
port object eq www
port-object eq smtp

show run object-group
```

ACLs

ASA use network mask instead of wildcard (as is done with the integrated router). ACLs are named and not given a number (as is done with the integrated router). Without an ACL configured, ASA works with security levels (lower levels cannot reach higher levels). Standard ACL inspect only source address, extended inspect source, destination, port and protocols.

```
help access-list

access-group ACL-IN in interface outside
show running-config access-list
show access-list ACL-IN breif
```

It's easier to create an extended ACL with object groups.

Dynamic NAT

Types supported are Inside NAT, Outside NAT and Bi-directional NAT.

```
object network PUBLIC
range ...
object network DYNAMIC-NAT
subnet 192.168.1.0 255.255.255.254
nat (inside, outside) dynamic PUBLIC

show xlate
show nat detail
```

Dynamic PAT

```
object-network INSIDE-NET
subnet 192.168.1.0 255.255.255.254
nat (inside, outside) dynamic interface

show xlate
show nat detail
```

AAA (TACACS+)

```
username Admin password class privilege 15
show run username

aaa-server TACACS-SVR protocol tacacs+
aaa-server TACACS-SVR (dmz) host 192.168.2.3

aaa authentication http console TACACS-SVR LOCAL
aaa authentication enable console TACACS-SVR LOCAL
...
aaa authentication telnet console TACACS-SVR LOCAL

show run aaa-server
```

Week 6

System Testing & Evaluation (ST&E)

- Uncover design, implementation and operational flwas that could to to the violation of the security policy.
- Determine the adequacy of security mechanisms, assurances and device properties to enforce the security policy.

Types of test

- Penetration testing
- Network scanning (port-knock, UDP scanning etc.)
- Vulnerability scanning (what vulnerabilities are available)
- Password cracking (default passwords / weak passwords / dictionary attacks / rainbow tables)
- Log review (most important! Monitor all events in a network)
- Integrity checks (file system integrity / monitoring / login logging)
- Virus detection

Applying network test results

- Define mitigation activities
- Use as benchmark
- Assess implementation status of security requirements
- Cost and benefit analysis

Usable tools

- NMap / ZenMap (network mapping / scanning)
- SuperScan (Microsoft's scanning framework)
- SIEM (Security Information Event Management - real time reporting / forensics)
- GFI LANguard
- Tripwire (Testing TCP / UDP / ping sweep / find faulty configuration)
- Nessus (Famous software / vulnerability scanner - good!)

- L0phtCrack (Password cracker)
- Metasploit (Penetration testing framework)

Security Policy

1. Identifaction and authentication policies
2. Password policies
3. Acceptable use policies
4. Remote access policies
5. Network maintiance procedures
6. Incident handling procedures

Hierarchy:

| ———> Techical policies

Governingpolicies - -|

|———---> End User policies

Governing Policy

- Statement of the issue that the policy addressess
- How the policy applies in the environment
- Roles and responsibilities

Technical Policy

- General policies
- Telephony policies
- Email and communication policy
- Remote access policy
- Network policy
- Application policy

End User Policies

Customize End-User Policies for groups. Customers, empolyees, partners.

Standards

What OS, tools, languages etc. to use.

Flight Check List

Step by step what needs to be done before work can be started.