Alpha Team Security Policy Documentation

Organization: Clothing Brand (Machina)

Name: Treymon Dentman (Security Specialist)

Team Members: Aaron Foster, Marquis Buckley, Iguodala Christian, Jerry Edose

Date: 11/19/2025

Overview

This report outlines the design and implementation of a secure network for our Clothing Brand Business (Machina). It also explains the reasoning behind the network topology, key findings, and the main security objectives.

Purpose

The purpose of this security policy is to protect the integrity, confidentiality, and availability of the company's corporate network and its data across all departments: Corporation, Marketing, Sales, Design, Manufacturing, and Supply.

Network Structure

Internal Network

- **Router 1 – Corporation Department:** 1 switch, 1 server, 1 laptop, 1 desktop
- **Router 2 – Marketing Department:** 1 switch, 2 desktops
- **Router 3 – Sales Department:** 1 switch, 2 desktops
- **Router 4 – Design Department:** 1 laptop, 1 desktop
- **Router 5 – Manufacturing Department:** 2 laptops
- **Router 6 – Supply Department:** 2 laptops

External Network

- **Router 1 – Corporation Department:** 1 internal router, 1 internal switch, 1 external router, 1 external switch, 1 firewall, external users/browser

Security Foundation

- Restrict data access to authorized users to protect confidentiality.
- Maintain network availability by preventing disruptions or unauthorized changes.
- Protect data integrity by blocking unauthorized access or alterations.

Security Policy for Users

- Users will browse through HTTP with VPN allowed.
- Users may create shopping accounts with a username and password.
- Optional two-factor authentication will be available.
- All purchases will use safe and trusted encryption.

Security Policy for Company Employees

1. Access Control

- Each department will use a unique VLAN to isolate traffic.
- Employees must authenticate with unique credentials; passwords change every 6 months.
- Role-based access portals will be implemented. For example, Marketing cannot access Supply. Corporate is the main admin for access permissions.

2. Firewall & Router Security

- All routers require strong, encrypted console and enable passwords.
- Access Control Lists (ACLs) will restrict inter-department communication unless permitted.
- Only the Corporation Department's server will host centralized resources and backups.
- The Corporation server requires SSH for remote management. Telnet/Remote Desktop is disabled unless allowed by IT.
- Regular backups must be securely stored.
- Only authorized IT staff may have administrative privileges.
- All desktops and laptops must have updated antivirus software and host-based firewalls.
- USB storage on internal devices is restricted unless approved by IT.

Physical Security

- Networking equipment must be stored in secure areas with limited access.
- Laptops must not be left unattended in public areas.

Incident Reporting and Monitoring

- Router, server, and firewall logs will be reviewed weekly, and daily if suspicious activity occurs.
- Unauthorized access attempts must be reported immediately.

Enforcement

Employees who violate this policy may face disciplinary action, up to and including termination of employment. Anyone who tampers with or any unlawful actions will be subject to prosecution.

Policy Reviews

This policy will be reviewed every 6–12 months or after any major network update.

My Additives / Findings

During development, each department was designed as its own “router” in the topology, though they operate as VLANs. This reduces traffic and allows quick isolation if a threat actor appears in the network. Departments cannot communicate or grant admin permissions except Corporate.

For the external network, an additional line for users to shop was added, including two routers (internal and external). This required updates such as a firewall and internal/external switches. The firewall was assigned a hostname, username, and password for exclusive management.

Configuration steps included identifying the gigabit interfaces (gig 1/1 and gig 1/2), connecting them to the appropriate switches, and assigning IP addresses from the internal and external routers. Interface gig 1/1 received an internal security level of 100, and gig 1/2 was set as DMZ with a security level of 70 to allow partial trust for external traffic. The cloud (external user / browser) is what the consumers will be using to access store products which will be connected to external router (depending on their ISP).

The "no shut" command was applied to enable signal flow from the switches. A final check using "write memory" confirmed the firewall status was up and functioning.

Verification and Validation

```
PERIMETER-FW(config)#
PERIMETER-FW(config)#
PERIMETER-FW(config)#write memory
Building configuration...
Cryptochecksum: 230844a2 7290008b 6d9b5ec2 5ea03836

1191  bytes copied in 1.402 secs (849 bytes/sec)
[OK]
PERIMETER-FW(config)#
```

```
PERIMETER-FW(config)#username ZeroDayTre password ZeroDayTre
PERIMETER-FW(config)#sh Start
: Saved
: Written by enable_15 at 12:18:29 UTC Nov 19 2025
: Call-home enabled from prompt by enable_15 at 12:18:29 UTC Nov 19 2025
!
hostname PERIMETER-FW
names
!
interface GigabitEthernet1/1
 nameif INSIDE
 security-level 100
 ip address 10.0.13.1 255.255.255.252
!
interface GigabitEthernet1/2
 nameif DMZ
 security-level 70
 ip address 10.0.13.2 255.255.255.252
!
interface GigabitEthernet1/3
 no nameif
 no security-level
 no ip address
 shutdown
<--- More --->
```

Copy Paste