CYB430

2.2 Activity: Security Policies

Darius Artis, Brandon Brooks, Adam Wheeler, Nazir Terrell, Issa Nkulu

3/10/2025

To set up user zones the first step is to access policies -> security.

1. All users in the users zone should not be able to access any devices in the other subnets in the users zone.
   1. **To set up user zones the first step is to access policies -> security. (Policy Type: Internal “Intrazone”)**

Name: Block-Users-to-Users

Rule Type: Deny

Source Zone: Users

Destination Zone: Users

Source Address: Any

Destination Address: Any

Application: Any

Service/Port: Any

Action: Deny

1. All users in the users zone should be able to access Kerberos, and LDAP on Domain Controllers in the NOC zone.
   1. **To set up user zones the first step is to access policies -> security (Policy Type: Interzone)**

Name: Allow-Users-to-DCs

Rule Type: Allow

Source Zone: Users

Destination Zone: NOC

Source Address: Any

Destination Address: Domain Controllers (Specific IPs or Address Group)

Application: Kerberos, LDAP

Service/Port:

Kerberos: TCP/UDP 88

LDAP: TCP/UDP 389

Action: Allow

1. All users in the Users zone should be able to access all web servers in the Internet zone except those in Russia
   1. **To set up user zones the first step is to access policies -> security (Policy Type: “External” Interzone)**

Name: Block-Users-to-Russian-Web-Servers

Rule Type: Deny

Source Zone: Users

Destination Zone: Internet

Source Address: Any

Destination Address: Any (except Russian IP Address Range (Geo-IP-based blocking))

Application: Web-Browsing

Action: Deny