System Guide and Maintenance

for

Expense Tracker

PunchCards

November 18, 2008

CS451

University of Missouri – Kansas City

System Installation

1. Switches
   1. Connect an Ethernet cable into an outgoing port on your modem or router – sometimes marked as a “WAN” port (on a router – any port will do)
   2. Take the other end of the Ethernet cable and plug it into any port on your switch
   3. Now plug another Ethernet cable cable into another port on your switch
   4. Plug the other end of the Ethernet cable into your device
2. Firewall
   1. Connect the FortiGate’s Internet-facing interface (typically WAN1) to your ISP-supplied equipment.
   2. Connect a PC to the FortiGate using an internal port (typically port 1).
   3. Power on the ISP’s equipment, the FortiGate unit, and the PC on the internal network.
   4. From the PC on the internal network, connect to the FortiGate’s web-based manager using either FortiExplorer or an Internet browser (for information about connecting to the web-based manager, please see your models QuickStart Guide). Login using an admin account (the default admin account has the username admin and no password).
   5. Go to System > Network > Interfaces and edit the Internet-facing interface. Set Addressing Mode to Manual and the IP/Netmask to your public IP address. Select OK.
   6. Edit the internal interface. Set Addressing Mode to Manual and set the IP/Netmask to the private IP address you wish to use for the FortiGate. Select OK.
   7. Go to Router > Static > Static Routes (or System > Network > Routing, depending on your FortiGate model) and select Create New to add a default route. Set the Destination IP/Mask to 0.0.0.0/0.0.0.0, the Device to the Internet-facing interface, and the Gateway to the gateway (or default route) provided by your ISP or to the next hop router, depending on your network requirements. Select OK.
3. FireEye & Inky
   1. When we issue out the computers will be in our image for the machines.
   2. While in the user's email they will be able to make reports of phishing attempts, spam and other risky emails to the IT department for them to block by address, or IP.
4. VPN
   1. Download FortiClient from website
   2. Create User/User Group
      1. User & Device -> User Definition -> Create New
         1. Fill out information the system asks for
      2. User & Device -> User Groups -> Create New
         1. Fill out group name and add people to the group
   3. Configure IPsec VPN
      1. VPN -> IPsec Wizard
         1. VPN Setup
            1. Fill out VPN name
            2. Change template type to Remote Access
            3. Set Remote Device Type to FortiClient VPN
         2. Authentication
            1. Change Incoming Interface match your user’s interface
            2. Change Authentication Method to Pre-shared Key
            3. Enter the Pre-shared key
            4. Select user group
         3. Policy and Routing
            1. set Local Interface to an internal interface
            2. set Local Address to the local LAN address and create a local network.

name the local network

set type to IP/Netmask

set Subnet/IP Range to the local subnet

change interface to a local port on the LAN

* + - * 1. Enter a client IP address range
        2. Enter a subnet mask
        3. Disable IPv4 Split Tunnel
      1. Client Options
         1. Select the client options that fit your needs
  1. Create a security policy
     1. Policy & Objects -> IPv4 Policy -> Create New
        1. Name policy
        2. Set Incoming Interface to the tunnel interface
        3. Set Outgoing interface to match your user’s interface
        4. Set Source, Service and Destination Address to All
        5. Enable NAT
        6. Configure Security as needed
  2. Configure FortiClient
     1. Click Add Connection
        1. Add connection depending on location of the office
        2. Add the end users username to make it easier
        3. Once configured, they just need to enter their same password to connect and they have access to company drives.

System Maintenance

1. Switches
   1. Check LEDs
      1. The Power LED should be solid green (or blue, if clients are connected). If it is ﬂashing blue, the ﬁrmware is automatically upgraded and the LED should turn green when the upgrade is completed (normally within a few minutes). See the "LED Indicators" section for more details. .
      2. Note: Your MR42 must have an active route to the Internet to check and upgrade its ﬁrmware.
   2. Verify access point connectivity
      1. Use any 802.11 client device to connect to the MR42 and verify proper connectivity using the client’s web browser.
   3. Check network coverage
   4. Conﬁrm that you have good signal strength throughout your coverage area. You can use the signal strength meter on a laptop, smart phone, or other wireless device.
2. Firewall
   1. Go to <http://www.fortiguard.com/antivirus/eicartest.html> to download the test file (eicar.com) or the test file in a ZIP archive (eicar.zip).
   2. If the antivirus profile applied to the security policy that allows you access to the Web is configured to scan HTTP traffic for viruses, any attempt to download the test file will be blocked. This indicates that you are protected.
3. FireEye & Inky
   1. Perform a penetration test against your system.
4. VPN
   1. Connect to VPN to access company information from home.
   2. The VPN acts as if you are in the office but you are just at home.

Database and Backend

The physical database is created within the code and is implemented using the integrated SQL server CE 3.5 database. In order to use SqlCe functions you have to also call the system.LINQ library. The database is created in the DataManager.cs file and is accessed by the ReportDAOSqlImpl.cs file. Within this file there are the various SQL statements that are used to persist the data. The queries are implemented using SqlCeCommand object class in that we create a SQL string and place it in a command object that we can use throughout the code but only have to worry about one instance of the physical query being updated. Currently SQL is the only type that is currently being accepted but it is possible to add other types to parse data including XML or text files by simply adding an instance of that type in the factory. The database will be stored and backed up in the Azure environment allowing for easy back up, and accessibility for changes to be made.