Five Below / NetFortris – Circuit Turnup Process (WIP)

Project Overview:
Five Below will be installing new wired internet circuits through NetFortris at all retail locations. Many retail locations have existing wired internet circuits through a different partner, some retail locations do not currently have a wired internet circuit. All retail locations have a 4G connection (via Cradlepoint), either for backup in instances where a wired internet circuit is present or primary in instances where there is an existing wired circuit.

The following scope of work outlines the actions required by the on-site NetFortris technician on the day of cutover. At a high level, the technician will arrive on site, identity themselves and their purpose to the store manager, locate the newly installed circuit, test it, contact Five Below IT, work with them to connect the new circuit to Five Below's Meraki network equipment, and validate store functions.

Pre-requisites (equipment / information the technician needs):

- Carrier notes outlining where the modem was installed and the circuit ID on the modem tag
- Materials required to extend the circuit (if applicable) into the manager's office (cables, tools, ladder, etc.)
- IP information for the circuit (usable IP address(es), subnet mask, gateway)
- Windows laptop with Ethernet port
- Ethernet cable for testing
- Cellphone with data plan
- Label maker

Step-by-step circuit turnup process:

1) Technician will arrive on site and identify themselves to the MOD (manager on duty) as a technician from NetFortris here to perform an internet upgrade. Your arrival will be communicated to the MOD prior to scheduled date. If the manager has any concerns with providing access, the technician should email WANRefresh@fivebelow.com with the store number and the technician's contact information. Someone will reach out to the store to confirm the appointment is legitimate.
2) Technician will contact the NetFortris turn-up team to check in and obtain any information not already received as part of the pre-requisites (modem install location, handoff interface, circuit ID, IP information for testing).
3) Technician will locate the carrier-installed device (modem, router, etc), verify it is the new device and NOT the existing device based on the circuit ID, and validate power to the device.
4) **If the carrier device is already in the Five Below network rack located inside the store manager's office**, connect an ethernet cable to the handoff port of the carrier device, proceed to step 6, and test the circuit.
5) **If the carrier device is not in the Five Below network rack located inside the store manager's office**, the technician will investigate options to extend the circuit into the store manager's office. Options in order of preference:
    a. Extend the carrier's line into the manager's office and place the carrier device in the Five Below network rack inside the store manager's office

b. Extend a cable from the handoff interface of the carrier's device and terminate into an available patch panel port (FB to confirm specific details on this). Label that patch panel port 'Internet' and run a cable from that patch panel port to be used for Five Below's internet connection.

c. If the extension would require additional equipment (i.e. a lift or other hardware) to complete, investigate if an existing extension is in place for the current wired circuit. If that is the case, we can make use of the existing extension. NOTE: DO NOT MOVE THE EXISTING CONNECTION WITHOUT CONTACTING FIVE BELOW IT PER THE INSTRUCTIONS IN STEP 8.

6) Input the circuit IP information obtained from NetFortris into the laptop NIC, plug the cable from the carrier device handoff port into the laptop ethernet port, and validate an internet connection can be made using the newly installed internet circuit. Run the below tests and capture the information with screenshots for Five Below IT:

a. Open a command prompt and type ipconfig. Take a screenshot of the ethernet adapter configuration containing the IP address, subnet mask, and default gateway.

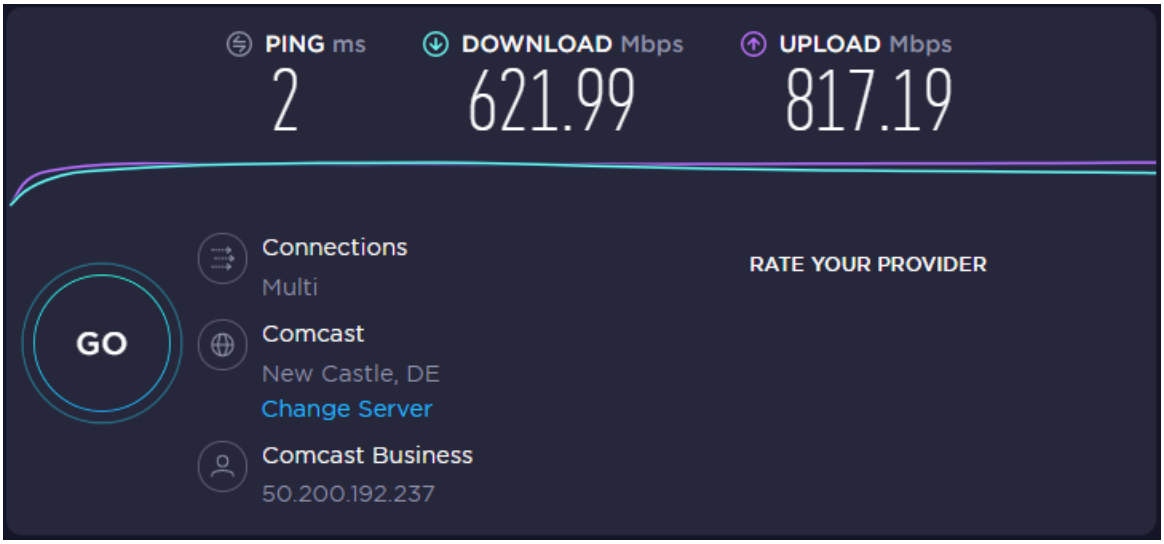
```
C:\Users\slaneyd>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 3:

   IPv4 Address. . . . . . . . . . . : 172.17.1.50
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.17.1.254
```

b. Browse to https://www.speedtest.net/ - once the page loads, select 'GO' to run a speed test. Once complete, take a screenshot of the results, example below:



7) If there are any issues obtaining a connection from the circuit, please engage the NetFortris turn-up team to validate the provided information is correct and have the issue investigated with the underlying carrier.

8) With the above information captured and a working circuit validated, please reach out to Five Below IT using the following e-mail template and the information captured above. Someone from Five Below IT will call the reach number provided and work with you on connecting the new circuit to Five Below's network equipment.
    - E-mail template (the e-mail must be sent to WANRefresh@fivebelow.com):
        - Subject line: Store XXXX (insert store number) – NetFortris Circuit Install
        - Body: Hello, the circuit at this location is ready to be turned up. Please contact me at your earliest convenience to connect and test.
            - Technician name: (insert name)
            - Technician phone number: (insert phone number)
            - Circuit IP information: (insert screenshot of ipconfig output)
            - Circuit speed test result: (insert screenshot of circuit speed test results)

9) Once the email is received, a Five Below technician will reach out at their earliest opportunity. Please allow ~15 minutes before sending a follow-up e-mail if you do not receive a call.
10) When connected with the Five Below technician, they will walk you through disconnecting the existing internet connection from the Meraki router, connecting the new internet circuit, and testing connectivity from the store. *** FB has internal documentation for the cut over process
11) Five Below to add details here – but the basic ask is that once cutover is complete, the technician remove the old modem/carrier device, box it up, label it, and inform the manager it needs to be kept in their office until further notice from IT. Again, we will align on an internal process and update this.

Endpoint Security Policy

Last Review: January 2021
Next Review: June 2021
Effective Date: January 1st, 2021

Presented by:

Tech Americas USA

Contents

Purpose

The purpose of this policy is to regulate protection of the customer network when accessed by Endpoint equipment such as laptops, tablets, and mobile devices. It is designed to protect our employees, customers and other partners from harm caused by the misuse of IT systems and data. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime.

Definitions

"Users" are everyone who has access to any of the Customer IT systems. This includes permanent employees and also temporary employees, contractors, agencies, consultants, suppliers, customers and business partners.

"Systems" means all IT equipment that connects to a corporate network or accesses corporate applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

Objective

The objective is to reduce the risk of security breaches that could result from the connection and use of Endpoint devices. This policy seeks to limit security threats by:

- Ensuring Users are aware of the requirements and restrictions around Endpoint devices.
- Enabling protective measures and controls to manage Endpoint security and software compliance risks.

Audience

Everyone who works at Tech Americas USA or anyone performing work on behalf of Tech Americas USA including contractors, consultants and volunteers are subject to this policy and responsible for the security of customer IT systems and the data on them. As such, everyone must ensure they adhere to the guidelines in this policy at all times.

Scope

This policy covers all Endpoint devices connected to any customer network.

Policy

This Audience is responsible for ensuring that:

Information Security

- All care is taken to prevent unintended exposure, modification, or removal of private, copyright, or confidential information as a result of leaving this information on the screen or desk, or exposed in such a way that it can be viewed or accessed by an unauthorized individual. This includes information stored on portable storage media or hard copy.
- Any private, sensitive, or confidential information that is stored on such an Endpoint device has the appropriate security controls to restrict and prevent retrieval or intercept by an unauthorized third-party.

End Point Software

All software contains security vulnerabilities, and software vendors are constantly supplying updates (patches) to address these vulnerabilities when they are identified.

- Endpoint software Operating Systems (OS) and application software are to be kept up to date with the latest security related patches, as soon as it is practical to do so, i.e.:
    - Critical security patches are applied within 1 week of them being released by vendors
    - Important security patches are applied within 2 weeks of them being released by vendors.
    - Endpoint systems must be restarted following installation, to ensure security patches have been fully installed.
    - Where possible, it is recommended that Endpoint devices are set to auto-update their security patch levels, and restart if necessary to complete the installation.

Computer and Data Security

If data on the Customer systems is classified as confidential users must take all necessary steps to prevent unauthorized access to confidential information.

Users are expected to exercise reasonable personal judgement when deciding which information is confidential.

Users must not send, upload, remove on portable media or otherwise transfer to a non-Customer system any information that is designated as confidential, or that they should reasonably regard as being confidential to the Customer except where explicitly authorized to do so in the performance of their regular duties.

Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices.

Multiple layers of security practices should be utilized for devices connected to the Customer systems. These layers include firewalls, up-to-date anti-virus software, current software security patches and spyware removal and detection software.

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into the Customer systems by whatever means.

All devices being connected to Customer systems should be for professional use and not contain personal documents or any have any content related to activities that are inappropriate for the Customer to be associated with and/or are detrimental to the company's reputation, including pornography, gambling, inciting hate, bullying and harassment.

Enforcement

Tech Americas USA will not tolerate any misuse of customer systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use. While each situation will be judged on a case-by-case basis, Users should be aware that consequences may include the termination of their employment.

Use of any of the customer resources for any illegal activity will usually be grounds for summary dismissal, and Tech Americas will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

Acceptance and Authorization

Performing service work by accepting a work order from Tech Americas USA implies acceptance of this policy. I have read and understand and agree to abide by its terms and conditions. I understand that violation of the use and provisions stated in the policy may result in limitations, suspension or dismissal, and/or disciplinary actions by Tech Americas USA or by legal authorities.