



Tk20 Network Infrastructure



**Your complete assessment
and reporting solution**

Tk20 Network Infrastructure

Table of Contents

- Overview 4
- Physical Layout 4
 - Air Conditioning:** 4
 - Backup Power:** 4
 - Personnel Security:** 4
 - Fire Prevention and Suppression:** 4
- Network Security: 5
 - Firewall:** 5
 - Virtual Private Network:** 5
 - Network Scans:** 5
 - Intrusion Detection System:** 5
- Network Architecture Diagram: 7
- Network Monitoring System: 8
 - Features of the Monitoring System:** 8

Overview

This document identifies the elements of the Tk20 Data center- its physical properties, network infrastructure, security and monitoring.

Physical Layout

The physical elements of our data center like power fail over, air conditioning, physical security and fire protection is rigorously controlled.

Air Conditioning:

Air conditioning to maintain a temperature range of 68-75 F is important for correct temperature and humidity to keep the servers and the internal components in good condition. At Tk20 we maintain such a system and also monitor these physical conditions using a temperature, humidity and water level sensor that can alert if any condition goes out of the accepted range. Refer to the monitoring system description on details of how any problem is handled.

Backup Power:

Tk20 Data Center has three phase power supply and each server is connected to at least two different phases to avoid single point failure.

Personnel Security:

Tk20 Data Center has restricted access to only the network administrators and support engineers at Tk20. This is achieved by using server rooms that have locked doors and monitoring of open door conditions using a closure contact detection sensor that alerts the network support engineers.

Fire Prevention and Suppression:

Tk20 Data Center is installed with smoke detectors to warn early about fire and in the event of a fire breakout installed gaseous fire suppression system can suppress fire faster without damaging equipment than manual extinguishers.

Network Infrastructure:

Tk20 production network has a bandwidth of two bonded T1 lines (3Mbps/sec). We have three different network lines that provide redundancy of internet connection and separate out live servers from internal Tk20 network needs. All hosted servers are behind the Tk20 firewall and a secure VPN system to reduce chances of intrusion. For network security purposes we have active and passive intrusion detection software.

Network Security:

The components of network security at Tk20 include Firewall, Remote Access using secure Virtual Private Network, passive network scan software and active network intrusion detection system.

Firewall:

Each sub network in Tk20 is behind a main firewall. This firewall blocks all requests except the protocols identified on ports that are used by the application software installed on the servers hosted and the ports that are used to provide operational support by accessing the servers. Firewall rules for remote access is restricted to three IP addresses that act as relay points and these relay servers can only be accessed after connecting to secure Tk20 VPN (see below).

Virtual Private Network:

Any remote shell access to a server for support and maintenance by Tk20 can happen only after connecting to the secure Tk20 VPN, enabling remote server shell connections to be encrypted and not accessible to the world. Most harmful attacks to servers happen through malicious shell access to a server that is open to the world and Tk20 VPN network prevents this. VPN network is password protected and accounts are provided to internal Tk20 support engineers, passwords are changed regularly and all network access goes through relay access points that can log access details. All Tk20 servers are behind the VPN network and firewall.

Network Scans:

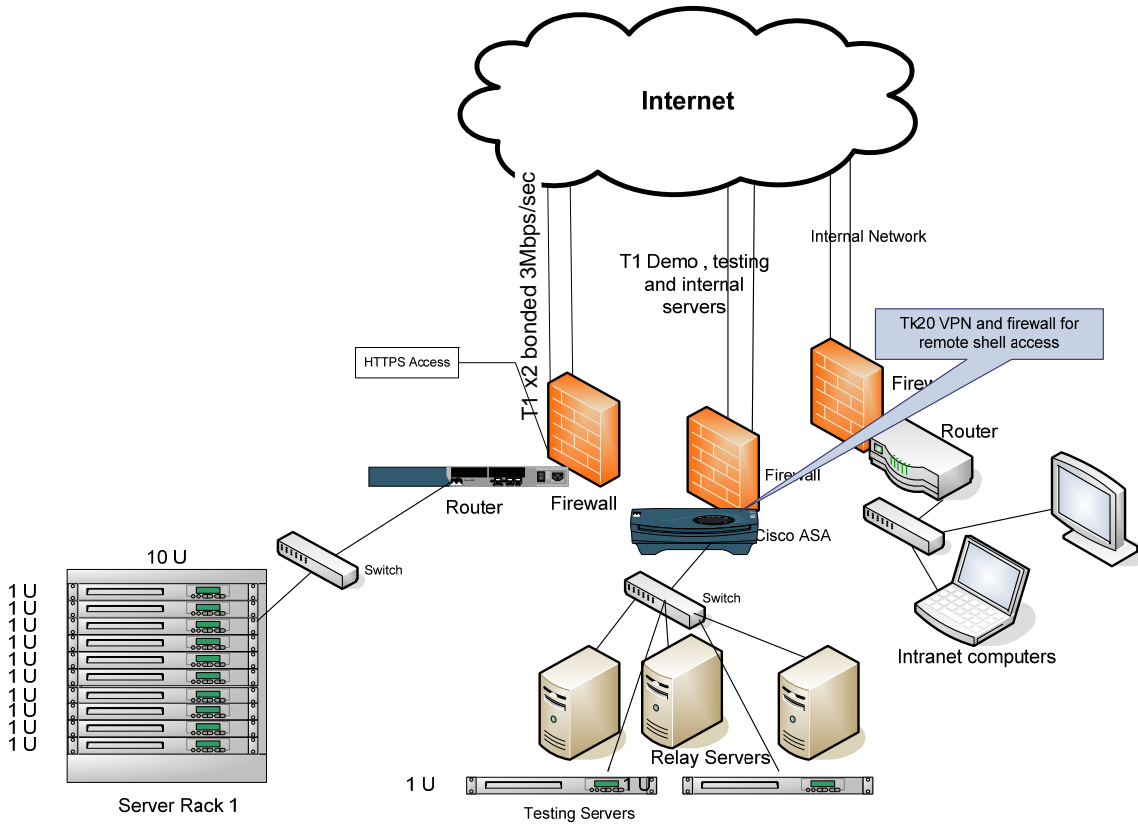
Network scan software called Nessus is used to run automated scans on all network servers to detect vulnerabilities in the operation system and application software installed on the servers. The master report is analyzed to take recommended actions to fix these vulnerabilities; these fixes include software upgrade of the operation system and third party software installed on the servers. The scan software is configured to download scan database updates to keep it up-to-date on known vulnerabilities.

Intrusion Detection System:

Tk20 uses Intrusion detection system software that resides on machine strategically placed to sniff on incoming and outgoing network packets. The hub to which it is

attached can smartly filter out known traffic for better performance and detect and alert malicious traffic attempts real-time based on its database which is updated automatically at a scheduled frequency.

Network Architecture Diagram:



Network Monitoring System:

Tk20 monitoring system consists of a centralized monitoring sever that runs regularly scheduled checks on hosts and services specified using external plugins which return status information to Nagios. When problems are encountered, the monitor can send notifications out to administrative contacts in Tk20 by a variety of different ways (email, instant message, SMS, etc.). Real time status information and historical logs can all be accessed via an authorized web page on the central monitoring server.

Features of the Monitoring System:

Tk20 central monitoring server has a lot of features that makes it a very powerful monitoring tool. Some of the major features are listed below:

- Monitoring of network services used by Tk20 (HTTP, PING etc)
- Monitoring of server resources (disk space and memory usage)
- Monitoring of software processes for application(java, postgresql, application access check etc)
- Contact notifications to Tk20 support when service or host problems occur and get resolved (via email, pager, or other user-defined method)
- Escalation of host and service notifications if a problem is not resolved within a configured time
- Scheduled downtime for suppressing host and service notifications during periods of planned outages
- Ability to acknowledge problems via the web interface so that Tk20 network support group is notified that someone is already working on the problem
- Central authorized web page for the network administrator to monitor network uptime and health of servers hosted