ITS Data Center Network Process

Service Offerings

The ITS datacenter team currently offers these services in the Durham and ASB datacenters:

- 1Gb (RJ45) and 10Gb (SFP+) and 40Gb (QSFP) ethernet
  - Servers only. We do not allow extension of the datacenter network by non-ITS managed switches or routers.
  - 40Gb interfaces are limited - please email us at its-datacenter-network@iastate.edu to discuss your 40Gb needs before purchasing network cards.
- Managed ASA services (to be retired by end of 2021)
  - Layer 3 / Layer 4 firewall
- Managed F5 services
  - port address translation (PAT)
  - DDoS mitigation
  - Layer 3 / Layer 4 firewall
  - Virtual IPs (VIPs)
    - Expose your application to the internet in a more secure manner
    - load balancing, if needed
    - application high availability services (active/standby, etc)

If there are additional services you’d like to see us offer, let us know.

Datacenter network redesign project 2019

Features of the new datacenter network design:

- Each college gets its own VLAN(s), one per data classification
- NAT can be enabled/disabled without re-IPing your device by submitting a firewall Service Request
- Public IPs are no longer assigned directly to servers
  - You can expose your application to the internet without having to re-IP from private/NAT
  - This change will allow implementation of next-generation firewall features at a later date
- Servers and applications will be firewalled by default
  - For servers and applications that would benefit from no firewall (i.e., high throughput applications), a firewall exception request can be started by emailing ITSecurity@iastate.edu
- Simplified troubleshooting of network issues
- Streamlined service catalog that will allow quicker implementation of service requests
- Workflows are designed to be self-service (via ServiceNow), to be implemented at a later date
- Full support for IPv6 (firewall support today, DHCPv6 support is coming)

What is the data classification policy?

Datacenter networks will adhere to the Data Classification Policy in accordance with the Data Classification Standards and Guidance document. In short, servers and services will be categorized and sorted into one of four data classes: Low, Moderate, High, and Restricted, based on the sensitivity of the data the server/service accesses. Security controls will be applied as appropriate. Servers of different data classes cannot exist together on the same VLAN.

How do I request service?

New application onboarding

“Application” is defined as a group of servers that share the following two items:

1. A similar set of firewall rules OR a common purpose;
2. A common admin team.
For new server/VM onboarding please email its-datacenter-network@iastate.edu and we'll walk you through the (still evolving) process. This document (IT Handbook) will act as the authoritative source for the evolving process and will be updated often.

When setting up a new application we'll ask for the following information:

- **Data class** - see the [Data Classification Questionnaire](#) to determine the appropriate data classification
  - Example: Based on the questionnaire my application is MODERATE.
- **Application owner team ASW list** (with Mail and Windows Active Directory Security Group properties enabled)
  - We'll use this list as a point of contact and to validate authorization for firewall changes
  - Example: The application is managed by the ITS Network team so use the its-datacenter-network ASW list to identify the owners of this application.
- **Application name**
  - Firewall rules will refer to this name.
  - Example: Please refer to this application as ITS-example-app.
- **Desired DNS names for:**
  - **Server**
  - **VIP (if applicable)** - if your application needs to be available from off campus without the VPN, your site's DNS will point to the VIP and not your server.
  - Example: Please call the server testserver1.its.iastate.edu and the public web site neteng-example.its.iastate.edu.
  - When we request the new IPs, what Net-ID should "own" them?
  - IPv4 and IPv6 addresses, only IPv4, or only IPv6?
  - ITS encourages IPv6 use if your servers/applications support it.
- **Admin access**
  - Which application and server administrators need access to the server for the purpose of administering the server or application?
    - **VPN IPs**
    - **Fixed address IPs**
  - What ports do those users need access to?
  - In some instances the admin access and inbound firewall ACL (below) will be the same.
  - Example: My admin team (consisting of netid.vpn.iastate.edu and netid2.vpn.iastate.edu) needs access to Remote Desktop in order to apply software updates to the application.
- **Inbound firewall ACL requirements for server**
  - Which ports do your users need access to on the server/VM? For web (HTTP/HTTPS) applications, TCP ports 80 and 443 are common.
  - Which IPs will your users be coming from? Should your application be restricted to a few VPN IPs, campus-only, or something else?
  - If access to your application is needed from the Internet we will provision a VIP for you.
  - Example: The users of my application will access my application from anywhere on campus port HTTP and HTTPS.
- **Inbound firewall ACL requirements for VIP** (if off-campus access to your server/Application is needed and VPN is not an option)
  - VIPs (virtual IPs) are configured on the F5 and provide non-campus access to datacenter-hosted applications, high availability, and load-balancing capabilities.
    - Which ports should be open? For web, 80 and 443 are common.
    - Which IPs need access to the VIP? Specific VPN IPs, specific servers, on-campus users, and the Internet are common choices.
  - Example: My public web site needs to be accessible globally (the entire internet) on HTTP/HTTPS ports.
- **Outbound ACL requirements**
  - For hosts classified Low, choose either:
    1. Outbound to campus, or
    2. Outbound to campus & Internet
  - For hosts classified Moderate, High, or Restricted:
    - Which on- or off-campus IP addresses does your server need to access, and on which ports?
    - Default outbound permits include: [ks.iastate.edu](#), ISU NTP, ISU DNS, [sus.iastate.edu](#), domain controllers, WINS, and [satellite.iastate.edu](#)
    - Example: My application sends HTTPS data to the off-campus web site example.com and gets HTTP updates from update.example.com.
Once the network team has this information we’ll assign IP addresses and ask you to submit ChangeGear requests in order to implement firewall and VIPs (if needed). We will provide the verbiage for those requests.

**Firewall rule add/update/remove**

Request a Firewall Change (via ChangeGear Top left corner -> Service Request -> +New -> Request a Firewall Change)

**Virtual IP (VIP) add/update/remove**

Request Load Balancer Services (via ChangeGear Top left corner -> Service Request -> +New -> Request Load Balancer Services)

- Add, modify, remove a VIP (Virtual IP)
- Add or modify a load balancing pool
- Add, update, or remove a TLS/SSL certificate from a VIP

**Other requests**

Send us an email at its-datacenter-network@iastate.edu if you have questions.

- Generic datacenter network add/change/remove (via ChangeGear Top left corner -> Service Request -> +New -> Request DC Network Services)
- For server hosting please contact the datacenter physical team (datacenter-requests@iastate.edu) or via ChangeGear:
  - ChangeGear Top left corner -> Service Request -> +New -> Request|decommission|modify a hosted server

**Datacenter network migration project**

**Goals:**

- Remove technical network debt (secondary networks, proxy arp) by retiring legacy networks (All datacenter networks not in VLANs 3300-3799)
- Implement data center firewall
- Segment servers based on college/division and data classification
- Provide consistent service through simplified workflows and standardized service offerings
- Reduce implementation time for deploying new servers, applications, and changes
- Reduce troubleshooting complexity
- Centralize and streamline request and change processes
- Promote use of IPv6
- Position us for implementation of next-generation firewall technologies at a later date

The ITS Network team is working to retire legacy datacenter networks, prioritizing existing non-firewalled networks (VLANs 6, 78, and 138, etc) before retiring existing firewall networks.

**Contact us**

Reach out to us at its-datacenter-network@iastate.edu with any questions or comments.

If there is a network issue please contact the Solution Center.