Information Services

Standing Service Level Agreement (SLA)
Firewall and VPN Services

Overview

This service level agreement (SLA) is between Information Services (IS), and any unit at the University of Oregon that makes use of the University's Centralized Firewall Services (UO-CFS). Under this SLA, Information Services agrees to provide access to the services outlined in this document, and the unit agrees to abide by the responsibilities and other requirements of the SLA.

This SLA documents agreed-upon systems and services, covers performance and reliability, targets objectives, outlines escalation processes, and serves as an invoice for financial transactions between parties.

Purpose

In support of the academic mission and administrative functions of the University of Oregon, Information Services will provide a fully managed and proactive firewall management solution where Network and Telecommunications Services (NTS) within IS is solely responsible for the administration, management, and monitoring of the firewall platform's configuration, security policy, and rule-set in accordance to this Service Level Agreement (SLA). NTS has dedicated staff that will work with authorized departmental security contacts to review, validate, implement, and audit firewall and VPN requests/changes as needed.

Duration of Agreement:

This standing agreement covers all virtual firewalls running on the Information Services' centralized firewall and VPN hardware, as well as dedicated standalone deployments. Any modification to this agreement will be posted to the Information Services' website at the following URL: http://security.uoregon.edu/firewallSLA/

Definition of Scope:

The hardware used to provide the standalone and centralized firewall and VPN services from the UOnet core is covered by this standing agreement. This includes core switching, routing, firewall, and VPN equipment. Building infrastructure and power systems not located in IS datacenters are not covered by this service level agreement.

Additional specific information regarding infrastructure and dependencies is available upon written request.

Implementation:

NTS will coordinate the deployment of firewall and VPN services either as virtual services in the University's centralized fabric or using standalone devices, depending on the user's needs. Building and core networking will also be handled by NTS and may include billable time and materials in order to provide connectivity to the firewall and VPN systems.

Maintenance periods:

NTS – *Firewall, VPN and network infrastructure maintenance will occur between 3am and 7am on Monday mornings or 5am-7am Thursday mornings.*

Typical work performed during systems maintenance periods:

- *Network upgrades or changes*
- *Software upgrades on network hardware*
- *Testing failover and other resiliency systems*
- *Changing or modifying firewall configuration (not including rule changes or normal non-service interrupting changes)*

Every effort is made to limit the impact of maintenance periods on service availability of production instances; however during the duration of regularly schedule maintenance periods, services running on hardware covered in this document may be unavailable. While the hardware described in this document may still be operational during these time-periods, firewall or VPN servers transport may be interrupted by unrelated network maintenance.

Notification of maintenance events will be sent at least twenty-four (24) hours in advance via uonet-outage@network-services.uoregon.edu or via direct email to the affected customer(s).

Duties:

Roles and Responsibilities:

Information Services – NTS manages all firewall and network hardware infrastructure related to the centralized firewall and VPN offering, this includes but is not limited to:

Service deployment

- Installation, maintenance, and configuration of new and existing hardware, software, and license codes
- Integration of firewall services into monitoring and alerting systems
- Provisioning of new firewalls and related network infrastructure
- Point to point VPN connections

- End-user VPN connections

Monitoring

- Core and edge device availability monitoring
- Performance monitoring of firewall and network hardware with timely communication to unit about performance problems or concerns with suggested resolution paths
- Log monitoring, analysis and archival

Maintenance and Operations

- Managing and processing renewal of all support agreements covering hardware and software related to the firewall and network hardware and related systems
- Rule-set validation, verification, tuning, and optimization
- Review of firewall policy and firewall security posture assessments
- Software upgrades, patch management and device configuration maintenance
- Device configuration change management and auditing
- Maintain backups of device configurations
- Comprehensive reporting upon written request

Emergency response and disaster recovery

- After-hours response to system outages by the NTS on-call staff
- Incident response related to disruptions of service from network or other related failures
- Network and firewall fault analysis and timely problem resolution

Unit Responsibilities:

- Reporting errors and connectivity or performance problems between systems with traffic traversing the firewall, including performance issues detected at the application level.
- Notifying NTS of changes in requirement needs with sufficient time to allow for adequate planning.
- Timely notification to NTS of changes to network infrastructure or protected systems behind the firewall, when these are not managed by NTS.
- Provide and maintain a list of contacts allowed to submit or approve changes for your firewall services. This list should be provided to the Security Group at security@uoregon.edu.
- Administration and troubleshooting of systems located behind the firewall
- Timely payment of any and all fees associated with administration or support related directly to the support of the unit needs and outlined within this document.

Change Requests:

Initial point of contact for all configuration changes will be via a work ticket in the *firewall* IT Helpdesk (Information Services' ticket tracking system) queue at firewall@ithelp.uoregon.edu or the NTS Hotline 541-346-4395. All changes to firewall configuration must be tracked in a work ticket. Changes will be made during normal business hours (8-5 Monday through Friday) unless prior arrangements are made with NTS, 24 hours in advance. NTS will make every effort to meet or exceed the following times for changes once all required information has been submitted through a work ticket:

Change	Completion Time
Access List (ACL) change	Within 1 business day
Provision new user VPN service	Within 3 business days
Add or modify authorized users from VPN service	Within 1 business day
Add or modify firewall zone	Within 2 business weeks
Configure point-to-point VPN service	Within 1 business week
Log analysis for application layer related issues	Within 1 business day

NTS reserves the right to refuse the implementation of a change if they determine that the change broadens the scope of service, or if they determine that it adversely affects other aspects of service availability.

Escalation:

Initial point of contact for all system availability problems will be via the *firewall* IT Helpdesk queue email address or via the NTS telephone hotline.

Incident Reporting and Escalation:

Tier 1: NTS – NTS Hotline or firewall ticket email address 541-346-4395 or firewall@ithelp.uoregon.edu

Tier 2: José A. Domínguez – Network Architect and Assistant Director for Network Engineering jad@uoregon.edu or 541-346-1685

Tier 3: Tony Saxman – Interim Director of Network and Telecommunications Services saxman@uoregon.edu or 541-346-8570

Tier 4: Melissa Woo – Vice Provost for Information Services and CIO (cio@uoregon.edu or 541-346-1702)

Service Expectations:

Users can expect approximately 99.9% service availability (Approximately 8.7 hours per year of unplanned outage time) for hardware and services covered by this SLA. This downtime is measured over the time period of a year, excluding anticipated outages and downtime performed during maintenance periods.

Service availability will be measured using Nagios service monitoring and records will be retained for one year. NTS will monitor the firewall and VPN physical devices as well as the availability of the individual virtual firewalls.

Overall system performance statistics will be monitored and graphed for a period of one year using SNMP. Currently NTS uses Cacti to graph and archive system performance data.

Service availability reports are available periodically by written request to NTS. Anonymized service availability information can also be provided during briefings to the UO IT community at departmental computing meetings, or to a target audience during Lunch & Learn sessions.

Penalties:

No penalty for missing this availability expectation will be enforced at this time. This service expectation should be used for planning purposes only.

Fees:

Required base service:

$125/month for the base firewall context license, one inside network zone and one outside network zone.

Additional services $41.66/month each:

- Additional firewall protected zone. This includes each physically separate IP network connected to the firewall, excluding the *inside* and *outside* networks included in the base service.

- Administrative VPN services. This includes both IPSec and SSL client VPN access. The VPN can be configured for split-tunneling or full tunneling. Only users identified as IT contacts for the covered department may use this VPN service.

- User VPN services. This includes both IPSec and SSL client VPN services for end-users. The VPN can be configured for split-tunneling or full tunneling. IT contacts for the department must provide and maintain a list of DuckID's that are allowed to use this resource on at least a quarterly basis.

- Point-to-point VPN services. This includes any and all point-to-point VPN connections that must terminate on the virtual firewall.

Costs to upgrade in-building and core networking equipment are not covered by these fees and will be negotiated on a case-by-case basis if necessary.

Total cost of the UO-CFS service will be prorated to twelve months and billed on a monthly basis along with the unit's telephone bill.

Organizational Code: _____ *Index:* _____

Accounting Contact: _____

Effective Date: _____
This agreement begins on the effective date and is considered a standing agreement, renewing yearly without action from either party until a signatory provides written notification of termination or change. NTS reserves the right to review service fees on an annual basis and adjust as appropriate.

Signature:_____	Signature:_____
Print:_____	Print:_____
Director of Unit Receiving Firewall Service	Director of Network and Telecom Services
Date:_____	Date:_____

Signature:_____	Signature:_____
Print:_____	Print:_____
Vice President or Dean of the Above Unit	Vice Provost and Chief Information Officer
Date:_____	Date:_____