Virginia Commonwealth University
Technology Services

Security Standards for Network Access Rules

Definition:	*This standard applies to the firewall rules that will be in effect for each of the multiple security zones implemented as Virtual Routing and Forwarding instances on the VCU network.*
Designation:	Technology Services Standard
Effective Date:	November 1, 2006
Review Frequency:	Annually or as needed
Authority:	VCU Chief Information Officer VCU Information Security Officer
In Compliance with:	VCU Academic Policy: Security of Network Resources VCU Academic Policy: Information Security Policy UITAC Goals*: Infrastructure Goal 3.* COV ITRM Information Technology Security Management Standard VCU Information Security Program Standards (based on SEC501-01) VCU Computer and Network Resources Use Policy

.

.

Current Environment:

RESNet:

1. All TCP and UDP traffic is allowed from the RESNet VRF to all other VCU subnets and to the Internet.
2. IDENT traffic is allowed to all VCU subnets and denied to the Internet.
3. DNS traffic is allowed to all VCU subnets and denied to the Internet
4. NetBIOS/SMB is filtered at the firewall between all RESNets and the rest of the university network.

VCUTemp:

1. All communications are currently allowed.

WirelessNet:

1. Access is currently restricted to the following protocols via logon to the Bluesocket gateway: HTTP, HTTPS, IMAP, secure IMAP, POP2, POP3, SMTP, secure SMTP and SSH. The wireless session is not encrypted.

Scope of Standard:

The requirements contained in this standard apply to firewall rules that will govern access for the multiple security zones or VRF (Virtual Routing and Forwarding) segments on the VCU network. The standard also applies to inter-VLAN security policies. The requirements specify the type of inbound and outbound traffic that will be allowed with regard to the Internet and other parts of the VCU network. These requirements take into consideration what is necessary to create a secure and safe operational environment for the users and devices contained within these VRFs by providing protection from security threats originating from the Internet and from within the internal VCU network. Only the exceptions for specific protocols and port numbers for each VRF or VLAN will be permitted in ACL (Access Control Lists) rules. All other traffic will be denied.

VRFs were created based on the requirements for functionality, the degree of secure access needed and the need for isolation from the external network (i.e., Internet) and the rest of the VCU network. Assignment to VFR segments is based on membership in a LDAP group. Security policies and firewall rules applicable to the VRFs are assigned and managed through the Firewall Services Module technology that is operation in the Cisco switch.

As part of this Standard, all changes to the Access Control Lists (ACLs) of network equipment must be logged and must go through a change management process.

Applied Industry Best Practices of:

- National Institute of Standards Technology (NIST)

Requirements of the Standard.

The following is a list of the VRF zones and the access rules specific to each zone:

1. **RESNet – covers all of the VCU Student Resident Network connections:**
    a. NetBIOS/SMB will be filtered in the FWSM RESNet context between all RESNets subnets and the rest of the university network. These protocols will be allowed between RESNet subnets.
    b. All inbound traffic initiated by Internet hosts will be denied.
    c. Inbound traffic from VCU network outside of the RESNet subnets will be permitted only for management traffic and ICMP pings.
    d. A connection limitation of 250 is allowed for each RESNet host.
    e. VPN traffic outbound from the RESnets will not be allowed.
    f. ICMP ping will not be allowed from the RESnet subnets outbound to the rest of the VCU network. Ping will be allowed to the Internet.
    g. Exceptions: IP access to hosts in the Office of Community Programs will be allowed since they are not part of RESNet.

2. **SECNet - for servers and workstations that contain or process sensitive data and require the highest level of security**
    a. Access from the external network (i.e., the Internet) will not be allowed except when connections have been initiated by the host on SECNet.
    b. Access from the internal network (i.e., VCU resources) will be limited to network management communications initiated from subnets used by authorized technical staff.
    c. FTP and Telnet and other insecure technologies are not allowed.

3. **SRVNet – for management of the internal VCU servers and other hosts that are not public facing**
    a. Access from outside the VCU network will only be allowed using VPN.

4. **VoIPNet – for Voice over IP requirements**

5. **MGTNet – for management of the network by VCUNet staff**
    a. Access from outside the VCU network will only be allowed using VPN. Some form of two factor authentication will be required in the near future.

b. Access from the internal network (i.e., VCU resources) will be limited to network management communications initiated by VCUNet analysts. Communications initiated from other subnets are intercepted by the firewall for user authentication to prevent denial of service against the end host. The protocols allowed are restricted to the following: telnet, SSH, HTTP, HTTPS, Radius, LWAP, SNMP, ICMP, Syslog and RDP.

6. **DMZNet – for management of servers and other hosts that are public facing**
    a. Ports 80/443 are not blocked inbound from the Internet.

7. **VCUTemp – for the internal VCU network where general users are located**

8. **WirelessNet – for the wireless network at VCU that is protected by VPN security.**
    a. Insecure access to the VCU Wireless network will be allowed with the full knowledge and understanding of the users.
    b. Secure access to the VCU Wireless network will be provided by VPN.

Implementation

The process for requesting new VRF segments will be developed and made available on the IT Professionals web site.

Enforcement

Only the settings for traffic, protocols and port access indicated in the firewall rules for each VRF zone will be permitted. All other traffic, protocols and ports will not be allowed.

All changes to the Access Control Lists (ACLs) of network equipment must be logged and must go through a change management process.

Exceptions

Requests for exceptions to the requirements of this standard should be made in writing (by hard copy or email) to the VCU VP/CIO.

Glossary

VRF (Virtual Routing and Forwarding) - is a technology that allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other. This technology is included in IP network routers and allows multiple instances of a routing table to exist in a router and work simultaneously. The functionality is increased by allowing network paths to be segmented without using multiple devices. VRF also increases network security because traffic is automatically segregated. In addition, VRF can potentially eliminate the need for encryption and authentication.

VRF acts like a logical router, but while a logical router may include many routing tables, a VRF instance uses only a single routing table. VRF requires a forwarding table that designates the next hop for each data packet, a list of devices that may be called upon to forward the packet, and a set of rules and routing protocols that govern how the packet is forwarded. These tables prevent traffic from being forwarded outside a specific VRF path and also keep out traffic that should remain outside the VRF path.

VLAN (Virtual Local Area Network) - is a method of creating independent logical networks within a physical network. Several VLANs can co-exist within such a network, which helps in reducing the broadcast domain.

A VLAN consists of a network of computers that behave as if connected to the same wire - even though they may actually be physically connected to different segments of a LAN. VLANs are configured through software rather than hardware, which make them extremely flexible.

MPLS (Multiprotocol Label Switching) - In an MPLS network, incoming packets are assigned a "label" by a "label edge router (LER)". Packets are forwarded along a "label switch path (LSP)" where each "label switch router (LSR)" makes forwarding decisions based solely on the contents of the label. At each hop, the LSR strips off the existing label and applies a new label which tells the next hop how to forward the packet.

Label Switch Paths (LSPs) are established to guarantee a certain level of performance, to route around network congestion or to create IP tunnels for network-based virtual private networks. An LSP can be established that crosses multiple Layer 2 transports such as Ethernet or ATM. Thus, MPLS has the ability to create end-to-end circuits, with specific performance characteristics, across any type of transport medium, eliminating the need for overlay networks or Layer 2 only control mechanisms.

FWSM (Firewall Services Module) – Cisco's solution that allows the securing of communications between VLANs on the same switch. This is a full PIX firewall on a card that fits into an available slot in a Cisco switch and uses the VLAN interfaces of the switch for ingress and egress of traffic. It takes advantage of port density and speed of the enterprise switch and supports throughput of up to 5.5Gbps. It uses the VLAN interfaces on the switch as its firewall interface so that policies can be created protecting hundreds of VLANs from each other with the full granularity of a PIX firewall. Virtual firewalls can be configured that allow management of separate policies.

ACS (Access Control Server) - Cisco Secure ACS helps to ensure enforcement of assigned policies by allowing network administrators to control many aspects of access including who can log into the network and privileges each user has in the network. The ACS is an important component of Cisco's Network Admission Control (NAC), which is an industry initiative sponsored by Cisco Systems that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. Cisco's ACS acts as a policy decision point in NAC deployments, evaluating credentials, determining the state of the host, and sending out per-user authorization to the network access devices.

Revision History: