Botany firewall policy

Prepared by Sean Shang

Oct 28, 2011

1. Botany network topology structure

Botany network has 4 sub-divided VRFs (virtual routing and forwarding network): BOTA-SECURE, BOTA-GENERAL, BOTA-SERVER and BOTA-DMZ. Each VRF is linked to an interface of the virtual firewall provided by UBC IT services. There is also an external interface link to the UBC campus network. A set of access rules can be applied to each interface/VRF to control or filter the network traffic that go in or out of the interface.
Botany also has 5 VLANs (virtual local area network). Each VLAN has different set of IP addresses. Among them, BIOL01-BOTANY2 and GRID2-BOTA-SERVERS VLAN are under BOTA-SERVERs VRF; BIOL01-BOTANY3 VLAN is under BOTA-SECURE VRF; BIOL-BOTANY-DMZ VLAN is under BOTA-DMZ VRF; BIOL01-BOTANY VLAN is under BOTA-GENERAL VRF.

2. Some firewall knowledge

2.1.1. System provider

The virtual firewall system we are using is provided by UBC IT Services, based on Cisco's FWSM (Firewall Service Module) platform configured in multiple-context mode. Multiple-context mode provides UBC IT with the ability to provision multiple unique firewall instances specific to every UBC department. This presents departmental IT administrators with the opportunity to firewall their networks at reduced cost, and without hardware maintenance.

2.1.2. Traffic direction

All access rules controlling network traffic have direction associated with them. The direction is relative to the interface that the access rule applied to. When the access rule is used to control network traffic initiated from inside VRF that attached to an interface, we call it an incoming rule applied to that interface. When the access rule is used to control network traffic target at the VRF that attached to an interface, we call it an outgoing rule applied to that interface.

2.1.3. Stateful packet filtering

Stateful packet filtering is the method used by the Cisco's firewall system. This technology maintains complete session state. Each time a TCP or User Datagram Protocol (UDP) connection is established for inbound or outbound connections, the information is logged in a stateful session flow table. The stateful session flow table, also known as the state table, contains the source and destination addresses, port numbers, TCP sequencing information, and additional flags for each TCP or UDP connection that is associated with that particular session. This information creates a connection object and consequently, all inbound and outbound packets are compared against session flows in the stateful session flow table. Return data is permitted through the firewall only if an appropriate connection exists to validate its passage.

2.1.4. Session Timeouts

Session timeouts are the time allowed for connections to exist before they are expired, and removed from the connection table. Once a connection is removed from the table, return traffic from a previously connected host will be denied access. The connection must be initiated again from the internal host.

3. Device allocation policy

All Botany Computers or other network devices will be allocated into 4 VRFs based on policy below:

3.1. BOTA-SECURE VRF

Computers to be located in this VRF must be maintained by Botany IT staff. Computers in this VRF should not run as any kind of server, and are not accessible from any other VRF or non-Botany network (unless closely monitored/controlled by Botany IT staff.).

Some other general requirements include:

- Must have anti-virus software installed;
- Anti-virus software must be updated automatically;
- Must have the most recent system updates installed;
- End user of the computer is aware of general security practice and using the computer as non-Administrator/non-root user.

For example: Botany Main Office staff computers.

3.2. BOTA-GENERAL VRF

This VRF is designed for all Botany computers that cannot be allocated into any other Botany VRFs.

3.3. BOTA-SERVER VRF

This VRF is designed for servers mainly accessed from computers within Botany network (such as Botany Main Office server) or servers accessed from small number of identified IP address (such as a database server accessed mainly from several computers in Beaty Biodiversity Research Centre). Computers in this VRF should not be used as desktop workstations for Word processing, email, web surfing, etc.

3.4. BOTA-DMZ VRF

This VRF is designed for servers accessed largely from computers outside of Botany networks, such as Botany Webserver. Again, Computers in this VRF should not be used as desktop workstations for Word processing, email, web surfing, etc.

4. Access rules

By default, each interface will block any incoming or outgoing traffic. Exceptions can be made by adding access rules for a specific IP address (or a group of IP addresses) in the VRF attached to that interface. The firewall system will not control network traffic within a VRF. Different set of access rules can be applied to the interface to which a VRF is attached. Access rules has two directions relative to the interface: incoming rules and outgoing rules. The general principles for different interfaces are listed below:

4.1. BOTA-SERVER

Servers in this VRF can access any non-Botany network and specific IP address in BOTA-DMZ VRF;

Only allow access from registered IP address (or a group of IP address) to registered port/ports of the server in this VRF.

4.2. BOTA-DMZ

Servers in this VRF can access any non-Botany network and specific IP address in BOTA-SERVER VRF;

Only allow access from registered IP address (or a group of IP address, or any IP address) to the registered port/ports of the server in this VRF.

4.3. BOTA-SECURE

Computers in this VRF can access any non-Botany network and registered IP addresses in BOTA-SERVER, BOTA-DMZ and BOTA-GENERAL VRF;

By default, computers in this VRF are not accessible from any other VRF or non-Botany network, unless closely monitored/controlled by Botany IT staff.

4.4. BOTA-GENERAL

Computers in this VRF can access any non-Botany network and registered IP addresses in BOTA-SERVER and BOTA-DMZ VRF;

By default, computers in this VRF are not accessible form any other VRF or non-Botany network, but the user can require Botany IT staff to make an exception by creating access rule/rules for the specific IP address. The request must clearly indicate all information listed below:

- Server type (such as Web server, FTP server, etc.);
- Server IP address;
- Server listening port/ports (such as TCP 22, TCP 443, etc.);
- Clients IP address (such as any IP address, single IP address, or a group of IP address).

5. Malicious behaviours

The firewall system provides tools for Botany IT staff to detect malicious behaviours against Botany network and computers. Botany IT staff is authorized to take necessary action to tackle the threat to Botany network. Some examples for identified malicious behaviours are:

- Port scanning
- Password cracking
- Denial-of-Service attack

6. Changes and updates for this policy

Botany IT staff will maintain this policy. Due to various reasons, such as technology evolutions, this policy may require changes or/and updates. Botany IT staff or any Botany members can require change or updates to this policy. Botany Head must approve the change or updates.

7. Note

Botany IT staff will not keep any firewall data log. Botany IT staff is not responsible to report any misusage of Botany and/or UBC computing resources.

This Policy is not intended to set forth an exhaustive list relating to the use of Botany computing resources. All users continue to be subject to all applicable laws and UBC policies (see UBC Policy Website http://www.universitycounsel.ubc.ca/policies/index.html).