NETWORK SECURITY ZONE STANDARD UPDATES

Architecture, Standards and Planning Branch
Office of the CIO ● Province of BC
People ● Collaboration ● Innovation

Version 2.0

July 27, 2012

Network Security Zone Standard Updates

This document summarizes changes that have been made in the Network Security Zone Standard since the July 27, 2012 vote.

Introduction:

The Network Security Zone standard will undergo a biannual review.

General Characteristics

- Changed datacenter zone extension requirement from dedicated fiber to dedicated private network facilities, and removed duplication.
- Summary now includes:
    - "All traffic that transits a security zone boundary must pass firewall rules, IPS and anomaly detection."
    - "All traffic that transits between zone C sub-zones must pass firewall rules, IPS and anomaly detection."

Detailed Characteristics and Standard

Management Plane

The management plane that is in the datacenter which is described in the Network Security Zone standard is specific to the management plane that is used for the administration of servers in datacenters. Future releases of the Network Security Zone standard will be expanded to include management planes used for the administration of workstations and network devices. Other management planes exist for backups, and the management of other devices.

DMZ

Servers and application residing within the DMZ are Internet accessible and require tighter host and application than Zone A and Zone B servers. Internet facing applications must undergo an Application Vulnerability Scan prior to be placed in the DMZ.

Servers cannot be in IDIR domain if they are in the DMZ. Servers in the DMZ are in the .DMZ domain. A trust relationship exists between IDIR and the DMZ.

Zone C

Zone C may be sub-divided into additional zones.

- Trusted – For IDIR users logging on to the network from a managed device.
- Semi-trusted – For IDIR users logging on to the network from an unmanaged device (including BYOD).
- Untrusted – For non-IDIR users accessing the network from an unmanaged device.
- BUS – The Building Utility Services network is for building control systems.

Security controls between the Zone C sub-zones must include firewall, IPS and anomaly detection.

Servers

Servers, both dedicated and virtual, can reside in only one non-management zone. A server may not exist in both the High Security Zone and the DMZ at the same time. Virtual Servers sharing a common Hardware or Virtual Operating System must reside on the same Zone.

Switches

Access and virtual access switches can reside in only one non-management zone. A switch may not exist in both the High Security Zone and the DMZ at the same time. Virtual Switches sharing a common Hardware or Virtual Operating System must reside on the same Zone.
Core and aggregation switches may reside in more than one zone.

Inter-zone Connectivity

With regard to Table 3, IP and Port #'s are mentioned, but not protocol's (TCP/UDP). Some traffic does not have port's, such as the ICMP protocol and various router protocols.

Enforcement

Zone B Access to the Internet

Some applications will require access to resources on the Internet. License validation and downloading application updates are examples where applications may require access to the Internet. Due to the dynamic nature of content distribution networks it may be difficult to identify specific IP addresses or even network ranges that need to be accessed by a specific application, therefore it is desirable to filter Internet traffic outbound from zone B based on URL. This may be accomplished by using the SSBC provided forward proxy service. In the event that an application requires Internet access and cannot be configured to use the forward proxy service, then the public IP address must be obscured using NAT.

- The default for zone B applications is No Access to the Internet.
- Applications that require access to the Internet from zone B should be deployed in such a way that the application owner leverages a proxy server in the DMZ.
- Access to the Internet for applications from zone B for applications that use HTTP or HTTPS may use the SSBC forward proxy service.

- In the event that an application is unable to use the SSBC proxy service and the application owner deems that it is impractical to host their own proxy service in the DMZ, then the application owner may request that SSBC grant an exception to allow the specified zone B application access to the Internet. The exception process differs from the exemption process.
- The exception request must include the name and IP address of the application. The name, telephone and email address of the application owner. Confirmation that the application requires Internet access and that the proxy service has been ruled out as an option and the reason for ruling out the proxy service as an option. Additionally the application owner must specify a destination port and IP address range that are required for their application.
- There will be no Zone B firewall rules that have a destination of any.
- In the event that an exception is made for a Zone B application the server's IP address will be NAT'd.

HP-AS defines firewall rules as requested by administrators. The information asset owner for the destination of firewall rule request is the approver and also responsible for ensure that firewall requests comply with this standard.