mancalanetworks
making networks manageable

Security one pager

Firewall evolution

Firewalls have progressed from being stateless to stateful, to performing deep packet inspection. Only the Network Controller uses configuration data, realtime tracing, and correlation to protect your organization from more complex attacks.

Firewalls protect networks from internal and external threats. They do this by selectively permitting or denying network traffic. Firewalls do not track network configuration, however, and are therefore vulnerable to a number of attacks.

> Stateless Firewalls

The first network firewalls were “stateless”. Each packet was treated in isolation, without correlating multiple packets across long-lived sessions. This limitation meant that attackers could craft packets which passed through the firewall, but which a host or application would treat as invalid for a particular session.

This limitation meant that the hosts which were “protected” by the firewall were in fact vulnerable to certain kinds of invalid traffic from the attacker.

> Stateful Firewalls

A stateful firewall performs inter-packet data tracking to monitor long-lived sessions. This tracking enables the firewall to block packets which do not match any existing session, or which are invalid for an existing session. This capability lets stateful firewalls provide better protection against a wider range of attacks as compared to a stateless firewall.

The limitation of stateful firewalls is that they inspect only the network transport portion of packets, and blindly pass all application data. End hosts “protected” by a stateful firewall were still vulnerable to attacks at the application layer, such as viruses transmitted over the HTTP.

> UTM Firewalls

A UTM firewall scans the application data for a session in order to perform virus detection or intrusion prevention. They may also provide application protection by enforcing the correct data format for each application, and blocking non-compliant data.

Due to the location of a UTM firewall, hosts in the network are still vulnerable to a wide range of attacks, such as traffic that is internal to the network and which therefore bypasses the firewall. For example, hosts that continue to use their DHCP lease after it has expired are in violation of corporate policy. Since the UTM firewall does not monitor the DHCP configuration or state of the DHCP database, it will pass traffic from the non-compliant host. Similar vulnerabilities exist with most protocols.

> Summary

The Mancala Network Controller monitors internal network traffic and configuration in order to maintain a coherent state of the network. This state includes information such as user location, “private” versus “public” addresses, DNS names, equipment location, etc. This tracking provides a real-time view of the state of network, and is used to increase security by better enforcing network policy. The result is an ability to discover and prevent attacks which existing security systems pass transparently.