The need for context aware network control

Five years ago, the key issues for network architects were in the backbone, ensuring the bandwidth and redundancy to deliver on SLAs. Today the key challenges are at the network edge.

The fast-growing number and diversity of devices needing support, the penetration of non-standard user-owned prosumer devices, and the deployment of new technologies such as desktop virtualization place growing stress on key elements of the classic network management model.

The starting point for most devices connecting to the corporate network is a DHCP request. An appropriately configured server responds with an IP address, routing and DNS parameters, and the new end-point is ready to network. When the network consisted essentially of fixed desktop PCs, this approach raised few issues.

Today business users expect to walk into any corporate office with their laptop, smartphone and tablet PC – company issued, or the user's own device – and get connected.

Managing who has access, and under what conditions, is an increasingly complex task.

Network architectures are reaching a breaking point trying to reconcile flexibility and productivity for end-users with the increasingly demanding requirements of information security and regulatory compliance regimes.

An analogy can be drawn between today's network security tools and processes and an air traffic control system that is limited to in-depth post-mortem analysis of why two planes on different bearings at the same altitude collided - important information, but insufficient to prevent the loss of life and property.

What is required in today's complex network architectures is a real-time situational awareness capability or "context aware network services" that enables counter measures to be deployed to prevent catastrophe.

CONTEXT AWARE SECURITY INSIDE THE NETWORK

Firewall-based network security architectures are based on protecting the known “good” corporate network from the threats of the “unknown” internet by filtering inbound (and, to a lesser extent, outbound) traffic. Increasingly sophisticated and costly technologies – VPNs, deep packet inspection, intrusion prevention, application layer analysis – are deployed in an ongoing war against ever more subtle attack techniques.

All of which overlooks two key elements for effective security of enterprise networks:

- **If you don’t know what you’re protecting, you can’t optimize your security policy.**
- **Perimeter protection is no defense against insider attacks.**

Laptops, tablets and smartphones are replacing desktop PCs as users go mobile. Peripheral devices such as printers and photocopiers need internet connectivity to send status and billing information to the service provider. VoIP phones, virtualized application environments, telepresence systems – each have their own specific connectivity requirements and their own security vulnerabilities.

A traditional firewall or UTM appliance, filtering according to IP addresses and protocols, applies the same security policies to a printer sending a maintenance message to the service provider, a group of users participating in a webinar and an iPhone user browsing YouTube. Because security appliances cannot identify and classify different end-point devices, differentiated security policies require time-consuming, error-prone manual rule generation, with updates required every time a new device is introduced or deployed.

The Network Controller delivers “layer 0” security by identifying and classifying every end-point device on the network. Using information published by the device in its core service dialog (DHCP, ARP, DNS, RADIUS, SIP) and correlating it with additional analysis of the device’s network traffic and behaviour, the Mancala Network Controller can accurately profile devices and users to facilitate the deployment of fully optimized security policies.

SECURITY AND FLEXIBILITY RECONCILED

Typical security deployments today leave the corporate network vulnerable to attack. End-point churn – the result of mobility and the shorter life-cycles of new portable end-points – makes locking-down the network to pre-identified devices impractical. Increased diversity in types of end-point devices and the protocols and traffic patterns they generate make it more and more difficult to design and maintain rules-based firewall security policies.

The Mancala Network Controller unifies visibility of users, devices and network events with an innovative, real-time enforcement capability.

With a coherent view of the current network state, it ensures the strict application of security policies based on network events detected by the controller and enterprise security policies.

WHY TRADITIONAL NAC IS NOT THE ANSWER

Network Access Control solutions, or NAC, emerged as a response to the issue of mobile users connecting potentially compromised laptops to the corporate network. The core features of a NAC solution should allow the network manager to control who connects to the network; to verify the machine is uninfected, and OS, antivirus and other security elements are clean and fully patched; and to quarantine unknown or non-compliant systems.

Vendors have taken multiple different approaches to this, typically depending on the vendor's own core competence. An anti-virus vendor's NAC, for example, bears little resemblance to a network hardware vendor's NAC. Dependency on additional products from the same vendor or qualified partners to complete the NAC architecture results in vendor lock-in – sometimes extending beyond the NAC product itself.

Many NAC products rely on interaction with network switches and routers to configure VLANs on the fly, or to apply access control lists to individual ports. This approach works in a hit and miss fashion dependent on model and firmware versions. Some manipulate network control protocols to achieve results, making network troubleshooting extremely difficult. Real world networks require a flexible solution that can mix and match enforcement techniques based on the network context in which it is deployed - the Network Controller.

Ultimately, however, NAC products are being overwhelmed by the diversity of devices connecting to today's networks. Designed to verify and authenticate PCs and laptops, they are now faced with smartphones, tablet PCs, IP telephones, IP cameras, hosted VMs on end-point devices – and new classes of devices are on the way.

Traditional NAC solutions are doomed to failure as a direct result of their lack of real-time situational awareness of network attached devices and network topology.

A STEP-BY-STEP APPROACH TO IMPROVING NETWORK SECURITY

1 The Mancala Network Controller offers an agent-less, non-invasive approach to more effective network security. Deployed on the network in learning mode, the Network Controller has no impact on end-users. Data collected by the Network Controller gives the network manager full 360° visibility of all devices connected to the network, an essential element in developing appropriate security policies.

2 Configuring the Mancala Network Controller as a relay for core services delivers a new level of situational awareness and control of the network. Rogue devices or end-points masquerading as other devices are easily detected. Depending on enterprise security policies, unknown devices can be locked out of the network, quarantined, or redirected to a captive portal for authentication while internal threats are mitigated by defining good behavior and blocking the bad (e.g.: VoIP phones don't connect to WikiLeaks, PCs don't communicate directly with VoIP phones,...)

3 Building on these starting blocks, additional features of the Mancala Network Controller deliver continuous improvements in agility and security to the network manager, supporting a network driven by business needs, not vendor technology.

Device centric, situationally aware policy enforcement such as provided by the Mancala Network Controller is the only reliable way to easily secure a network from unknown devices and a growing number of internal threats.

Mancala Network Controller - Enterprise network control and management solution

Built from a patented and award winning technology, the Network Controller's innovation lies in its capability to not only monitor network control flows, but to also leverage that information to increase network security and management flexibility.

The Network Controller is installed in the local network as a natural complement to routers, switches and firewalls already in place. It interfaces with the network control services (DNS, DHCP, RADIUS, SIP). Easily integrated into existing network infrastructure and solutions, it detects connected devices and users in real-time, analyses their behavior and acts automatically to optimize network security. It brings an unequaled combination of visibility and control to enterprise network environments.

The Network Controller is available in a range of software editions adapted to the specific needs of each vertical market : Enterprises, Systems Integrators, and Managed Service Providers. Optionally, the software solution may be preloaded onto a range of physical appliances.

Mancala Networks SAS
15 Avenue du Granier
38240 Meylan - France
www.mancalanetworks.com