Deployment Scenarios

The Network Controller can be used in a wide variety of network topologies. In this technical brief we describe the most common scenarios. The benefits and impacts of each scenario are described.

LOCATION

It can be difficult to know where to place a new type of device on the network. While the Network Controller adds new functionality to the network, it does so by leveraging existing and well-known topologies.

We assume that the initial deployment of a Network Controller is in a branch office. That office has one Network Controller either as a VMWare guest, or as a physical server in a server room. The Network Controller acts largely like any other device on the network. It has an Ethernet connection to the network, in order to interact with other devices.

The controller has full VLAN support, and can function on multiple VLANs at the same time.

While it can be deployed as a server providing network services in a branch office, the innovation of the Network Controller is in the proprietary data analysis and correlation engine. This engine allows it to detect topology and behavior state changes which are missed by existing monitoring systems. It also allows the product to produce warning and error messages based on these anomalous events.

The engine works with whatever information it has available. An initial configuration can be simply passive monitoring, for zero impact on the existing network. As the benefit of the controller is proven, it can be configured to have increased levels of interaction with the network. These additional interactions enable the Network Controller to produce a more detailed view of the network. This detailed view results in additional and more accurate alerts along with flexible capabilities to isolate and remediate devices that have violated policies.

The result is increased monitoring, traceability and control, with minimal change and minimal risk.

SCENARIO 1: PASSIVE MODE

In *Passive Mode*, the Network Controller requires minimal changes to the network, and generates as little traffic as possible. The goal is automated network discovery without change or interaction.

In operation, the Network Controller receives traffic from the span or mirror ports of local switches. Where possible, other broadcast traffic is also monitored.

All of this data is analyzed to build an inventory of devices that is up-to-date in real time. The data is correlated in order to check for consistency, and for anomalous behavior.

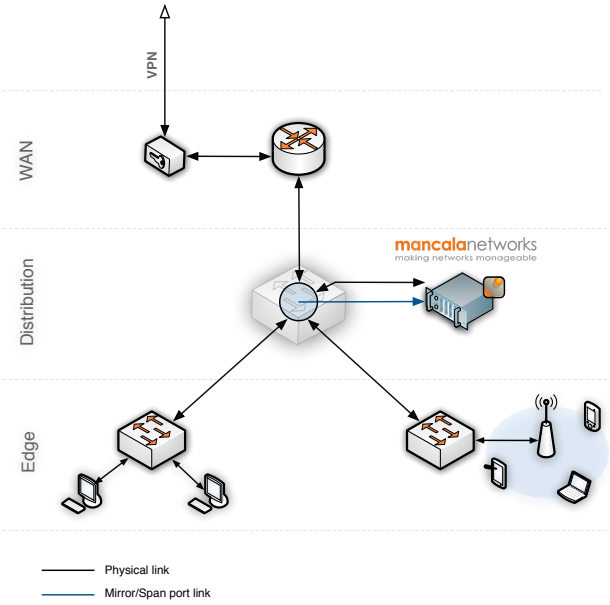

Fig. 1: *Passive Mode*

The result of this analysis is that the controller produces messages in real-time which describe the status of the network. These events can be used as input to a logging system, or to an Intrusion Detection System (IDS) where custom rules can be defined. Each event contains data about the kind of device on the network, and their behavior.

The administration interface of the controller can also be used to produce comprehensive reports about the network, and to view the topology in real time. The inventory that has been produced can be exported in industry standard formats, for import into existing configuration and asset management solutions.

Benefits: real-time inventory, traceability, and event notification of devices in the network. No changes to topology or network service configurations are required.

Impact: each switch needs to be configured to send span (or mirror) traffic to the Network Controller.

Limitations: the limitation of a passive monitoring system is that it does not interact with other devices on the network, and it does not take proactive steps to protect devices. Its responses are largely limited to sending alerts to an administrator and/or 3rd party SIEM solution.

SCENARIO 2: ACTIVE MODE

In *Active Mode*, the Network Controller pro-actively scans the network for new devices. It can also be configured to act as a relay agent for core services such as with DHCP and RADIUS to support user and device authentication as with 802.1X deployments. It can also act as a system controlling networks for both quarantine and remediation.

The purpose of deploying the Network Controller in *Active Mode* is to provide a gradual escalation of aggressive discovery and enforcement capabilities. While passive monitoring is good for non-intrusive configurations, a solely passive network discovery has limitations. Adding additional scans and enforcement increases the quality of the alerts, the enforcement capabilities, and the utility of the Network Controller.

We distinguish two types of *Active Mode* deployments. The first is *Active Scan*, where the Network Controller actively probes the network to discover new devices and to monitor state for existing devices. The second is *Active Response*, where the Network Controller makes decisions based on its policies, and takes independent action to protect the network.

Of course, the *Active Mode* functionality may also be combined in a hybrid mode with the passive functionality (scenario 1) described above in order to maximize the network visibility and policy enforcement capabilities.

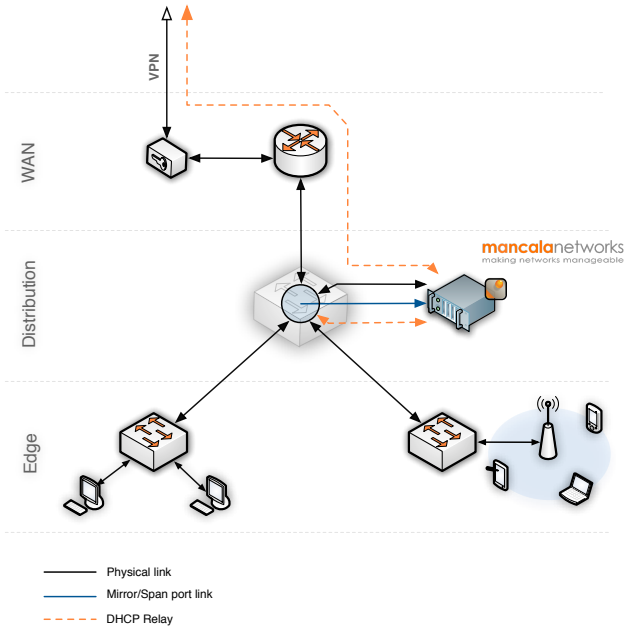

Fig. 2: *Active Mode*

ACTIVE SCAN

In the *Active Scan* deployment, the Network Controller is placed out of band of normal network traffic, but in a place where it can reach all of the devices in the network. It performs periodic, targeted scans of the network, and of new devices as they are discovered. These scans allow it to maintain a real-time detailed view of device type, location, operating system, and device activity. This information is used to generate alerts about anomalous behavior. It can also be used by third-party software (e.g. SIEM) to determine device status, in order for network-wide policy decisions to be made.

Where desired, switches can also be configured to forward RADIUS and/or DHCP traffic to the Network Controller. It acts as a pass-through relay to the existing services. The benefit of this relay behavior is that the Network Controller is notified in real time when changes occur on the network. While it forwards this information to existing services, it also updates its database to create a consolidated real-time view of every device.

Benefits: device posture assessment. Enables interpolation of data gathered by passive snooping, with data gathered by RADIUS and SNMP for a more complete inventory and network overview. Integration with Active Directory, LDAP or SQL allows deployment of user based access controls on Wireless Access Points and 802.1X enabled switches.

Impact: each switch needs to be configured to send RADIUS and DHCP traffic to the Network Controller.

ACTIVE RESPONSE

In the *Active Response* deployment, the Network Controller changes its behavior to enforce security policies. This enforcement is based on information discovered in the previous scenarios, and on policy rules defined by the administrator. The policies are unique to each state, and can be as detailed or as general as necessary. The policies can permit or deny traffic, and also permit or deny transitions to other states. This enforcement is done by modifying or redirecting network traffic, rather than by changing device configuration.

The result is increased manageability, with lower management cost and risk. For example, firewalls often have dozens or hundreds of complex filtering rules. In contrast, the Network Controller has a small number of powerful but easily understood rules, and a small number of easily understood network states. As devices enter the network, they are classified by type thereby enabling automatic application of specific policies by device type without cumbersome, manual intervention.

Benefit: actively enforces policies in real-time. Finds internal threats missed by other security devices. Protects core services and all internal systems from those threats.

Impact: minimal or no changes to configuration on existing RADIUS, DHCP or DNS services. May require additional configuration to allow it to obtain DNS and DHCP configuration from the existing services

CONCLUSION

The Network Controller can be used in a number of different deployment scenarios. This flexibility means that system administrators will see benefits when deploying the Network Controller in any possible architecture.

Mancala Networks recognizes that different networks have different needs and requirements. By making the Network Controller flexible, we ensure that it adds value in all possible situations.

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