DATASHEET

Model MCTNAC 2000

Network Access Control (NAC)

End-to-end security and superior user experience

NAC HIGHLIGHTS

BUSINESS ALIGNMENT

- Prevent unauthorized users, hacked endpoints, and other weak systems from connecting to the network in order to safeguard company data.
- Support 2000 endPoint
- Control the security posture of every device on the network, including employee-owned (BYOD) devices, proactively.
- Effectively handle the demands of regulatory compliance
- Protection at a reasonable cost for distant offices of businesses

OPERATIONAL EFFICIENCY

- Use already-existing software agents, authentication servers, assessment servers, and identity sources rather than forcing forklift upgrades.
- Give corporate employees the ability to quickly sponsor visitors and verify their registration.
- Use flexible deployment to safeguard both virtualized and physical environments, including virtual and real appliances.

Product Overview

MCT offers a comprehensive pre- and post-connect Network Access Control solution for wired and wireless LAN and VPN customers that is standards-based, multi-vendor compatible. IT managers can implement a cutting-edge NAC solution to guarantee that only the appropriate users have access to the appropriate information from the appropriate location at the appropriate time by using MCT Identity & Access appliances and/or Identity & Access Virtual Appliance with MCT NAC management configuration and reporting software. To offer the finest post-connect access control available, MCT NAC is tightly linked with the MCT Intrusion Prevention System (IPS), MCT EventShield(SIEM), and MCT Automated Security Manager.

Business-oriented visibility and control over specific users and apps in multi-vendor infrastructures is the MCT NAC advantage. Because NAC doesn't call for the installation of agents on every end system or the deployment of new switching gear, it safeguards the investments made in current infrastructure. MCT NAC carries out vulnerability evaluation, supported remediation, and multi-user, multi-method authentication. It gives you the freedom to decide how to treat authorized internal users and devices that fail the security posture assessment, as well as whether or not to re-restrict access for visitors and contractors to public Internet services exclusively. Companies are able to strike a balance between user security and efficiency. Users can choose to give themselves a grace period before being placed in quarantine, but the NAC assessment warning capability warns them when they need to upgrade their system.

Based on factors including device type, time and location, user identification, and other environmental variables, MCT NAC rules allow, reject, prioritize, rate-limit, tag, reroute, and audit network traffic. More potent isolation restrictions (which stop infected endpoints from launching attacks while in the quarantine state) on DevRay switches are supported by MCT NAC, along with RFC 3580 port and VLAN-based quarantine for both DevRay and third-party switches.

MapleCloud Technologies

Security

- With fine-grained access control based on user, device, time, location, and authentication type, you may provide the highest level of protection.
- Use agent-based or agent-less assessment to check end systems of any kind for risks or weaknesses.
- Automate continual threat analysis, containment, and prevention in addition to endpoint isolation, quarantine, and cleanup.

SERVICE & SUPPORT

- First call resolution and customer satisfaction rates that lead the industry
- Personalized services, such as site evaluations, network design, setup, and instruction

Any device that uses RADIUS for authorization and has customizable RADIUS characteristics, such Login-LAT or Filter ID, can use MCT NAC. Different rules may be implemented by enterprises based on the RADIUS reject property. As an illustration, a Users who have expired passwords could be subject to different policies than those who never had an account. With the most authentication choices available, the system enables unparalleled interoperability and supports Layer 2, Layer 3, and VPN access protocols.

The uniform setup of rules across various switch and wireless access point suppliers is made possible by MCT NAC. This feature facilitates the implementation of NAC and greatly lessens the workload associated with policy lifecycle management in heterogeneous infrastructures, wired and wireless Organizations may get instant network protection and business benefit with staggered deployment choices thanks to MCT NAC's flexibility. An organization may begin, for instance, with basic endpoint detection and location directory data, add authentication/authorization and/or evaluation, and then initiate remediation automatically.

Fine-Grained Configuration Options

MCT NAC configuration options offer unrivaled flexibility for fine-grained network control. Time, location, authentication methods, device and operating system type, and end system and user groups are among the configuration options available. Enterprises, for example, can create and implement policies that permit specific levels of network access based on the type of system connecting, an employee's job in the business, a user's location at the time of connection, or the time of day. Device and OS type regulations are especially relevant in workplaces where employees bring their own devices (BYOD). The organization can provide these devices network access that differs from what is authorized for corporate devices.

The network of an organization is more secure as access is restricted more strictly in terms of who can access it, when, and from where. These configuration choices' granularity also provide flexibility for effective deployment in sizable heterogeneous infrastructures.

Services for Guest Accounts Included

Secure guest networking is ensured by the automatic guest registration and access control capabilities of MCT NAC, all without taxing IT staff. Guest access control can be automated or delegated using NAC capabilities. Without involving IT, features like account validity and expiration regulate the guest account. MCT NAC includes sophisticated sponsorship features including email sponsorship and a straightforward interface for sponsors to utilize to verify visitor registration. It also allows customers to self-register numerous devices. Additionally, registration capabilities are offered for secure wireless guest access, which enables access to the network without the need for an 802.1X certificate or IT intervention, and automated contact verification by email or SMS.

MapleCloud Technologies

Dynamic role assignment for authorized registration is made possible via LDAP connectivity. Enterprise network users can register devices and assign the appropriate role to non-802.1X capable devices using authenticated registration. Administrators can grant varying degrees of access to different kinds of visitors by creating multiple registration groups. Guest access can be restricted to a particular connection point (SSID, port, switch) or set of related connection points using location-based registration.

Networking Aware of Identity

A user's capabilities are restricted in an identity-aware network according to their identification and the access policies assigned to them. User identification functionality, such as role-based access restrictions, authentication, and discovery, is offered by MCT NAC. Utilizing and expanding the company's current directory investments, MCT NAC interacts with identity sources including Microsoft Active Directory and Siemens Enterprise Communications HiPath DirX Identity. The identification system for the network and all linked apps manages users centrally. With LDAP and RADIUS connectivity, controlling the user lifetime (enrollment, role modifications, termination, etc.) may be automated and connected to other business processes. The organization has the option to automatically add or remove users upon their joining or departure.Stronger network security and lower operating costs are provided by MCT identity-aware networking features.

Baselining and Monitoring Endpoints

For control to be most effective, the network access control system should integrate with all end systems in the network architecture. To examine an endpoint's security posture, MCT NAC offers agent-based or agent-less endpoint assessment capabilities. In accordance with industry standards, MCT NAC adapts to the requirements of enterprises that might already have assessment technology by integrating numerous assessment servers, authentication servers, and security software agents.Usually applied to end systems like guest PCs, IP phones, IP cameras, or printers, the agentless feature eliminates the need for software security agents to be installed on the system. Operating system and application vulnerabilities are examined by the MCT agentless assessment. Installing a software agent on the end system is necessary for the agent-based functionality. The endpoint agent checks for peer-to-peer file sharing apps, operating system patches, firewall status, and antivirus software. The agent is capable of automatically fixing any process or registry entry that it finds. The MCT NAC solutions combination of agent and agent-less features makes management and reporting more effective.

Reporting & Notifications

MCT NAC's sophisticated notification engine offers extensive capabilities and synchronizes with the processes of other installed alerting solutions. Businesses can further save operating expenses by utilizing and expanding their current automated procedures. Notifications are sent out in relation to any modifications to custom fields, end-system health results, guest registration, and end-system additions or states.Notifications can be sent by email, web services, syslog, or traps. A program that is triggered by a notification event can be executed by the notification engine. For instance, NAC notification combined with the support desk application may be used to automatically map infrastructure changes to actions.

MCT NAC web-based end-system data displays make end-system reporting easy. Simple-to-use dashboards and comprehensive views of the condition of end systems connected to or attempting to connect to the network are offered by NAC. It is simple for analysts in charge of endsystem compliance monitoring to modify the views so that the data is shown in the way they choose. PDF files can be created from the reports.

Additionally, a crucial component of comprehending the network is end-system administration and monitoring. It gives administrators improved visibility, troubleshooting, and security by enabling them to comprehend the "who, what, when, where, and how" of the end-systems connected to the network. Currently, tracking end-systems just requires a search for a username, hostname, or address to locate all of their information, including the NetFlow data.

Integrations

Implementing Software Defined Networking (SDN) on any network is made easy, open, programmable, and centrally controlled with the help of the MCT OneFabric Connect API. Business applications may be monitored with NetSight and immediately controlled from OneFabric Control Center Advanced with OneFabric Connect. The final result is a comprehensive SDN solution that includes datacenter management, integrations with iBoss web filters, and several other products, in addition to integrations with the NAC solution such as MDM connectors with vendors like Airwatch, Mobile Iron, JAMF Software, and more.

MapleCloud Technologies

Additional Features

- Features for controlling "bring your own device" (BYOD), such as session-based user login and mobile device registration.
- Support for IPv6 in networks with IPv6 end systems to enable NAC installation.
- Verified compatibility with Trusted Computing Group TNC and Microsoft NAP.
- By detecting new MAC addresses, IP addresses, 802.1X / Web-based authentication sessions, or Kerberos or RADIUS requests from access switches, automatic endpoint discovery and position tracking may be carried out.
- All five NAC deployment models—intelligent wired edge, intelligent wireless edge, non-intelligent wired edge, and VPN—as well as Layer 2 deployment types are supported.
- MCT NAC offers VPN functionality and increases policy flexibility when used with an MCT SSA switch that is being distributed.
- By supporting external RADIUS load balancers, a group of NAC Appliances may have the load for handling authentication requests and setting switches distributed equally among the external load balancers.
- Options for management can be adjusted to fit current security specifications and network administration methods.
- The ability to identify the server to which a request is sent is made possible by support for various RADIUS and LDAP server groups.
- Support for agent-based evaluation using Macintosh agents.
- IT workflow integration is supported by open XML APIs, enabling automated, efficient processes.
- Integration with external programs is made easier by the web-service based NAC API.
- Layer 2 deployment configurations with 1 + 1 redundancy offer high availability and remove the Identity & Access application as a single point of failure.
- The risk level configuration gives you freedom in assessing the hazard the end system poses. The NAC administrator may establish High Risk, Medium Risk, and Low Risk criteria in accordance with local security regulations and concerns thanks to fine-grained control.
- Because MCT NAC is upgradeable, assessment and other NAC features may be combined onto a single machine. The appliances have the ability to provide evaluation that is agent-based or network-based.