Applying Network Security Monitoring to NAC

Successfully implementing effective Network Access Control at the enterprise level requires the ability to understand the behavior of individual hosts once they have been granted access to the network. Post-admission control policies must exist and various key elements of the enterprise network need to be connected in order to apply these access policies accordingly. Unfortunately many enterprises lack the necessary tools to truly understand how individual hosts behave once gaining access to the network.

QRadar, is the only product on the market with the ability to track and store both network and security activity; activity that is collected from device and host events as well as live network session data (or Flow information). Advanced analytics are applied to this network and security 'telemetry' to detect malicious or unwanted behavior from a particular host on the network. By adding support for TCG standards and integrating with Trusted Network Connect architecture, QRadar enables the enforcement of post-admission access control decisions when malicious or suspicious behavior is detected and correlated from information sources within the network.

Traditional NAC policies may require end points to be patched correctly, to have an AV client installed, and make sure that the latest AV definition files are downloaded. Once they are within the network substantial damage and downtime can occur if hosts that have passed initial NAC checks aren't subsequently monitored. QRadar has the ability to collect AV information, and then correlate this information to network flow data, firewall logs, and web proxy logs that are internal to the network in order to determine the nature of that host's activity. QRadar is then able to make a TNC recommendation to the Access Control device limiting the offending host's network access, or even removing the host from the network completely.

How does QRadar monitor the Network?

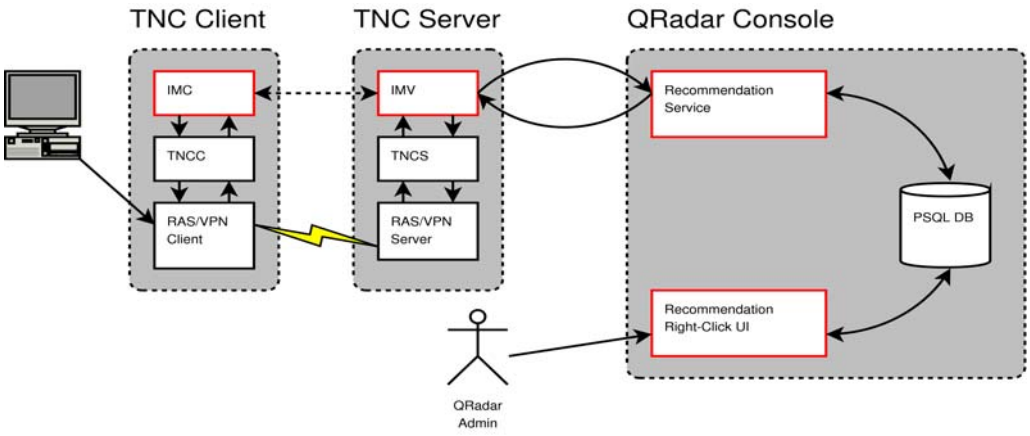
Successfully integrating what is understood about the network with what is observed in the security fabric enables a true security management solution. QRadar collects security events from a heterogeneous set of sources that includes network infrastructure, security devices, identity sources, servers and applications. It normalizes all events to enable automatic out-of-box correlation with other events and network flows. In addition to event data, QRadar also gathers vulnerability data to incorporate in asset profiles that are maintained for each business asset.

QRadar surveys the entire network, using native flow sources in a customer's routing/switching infrastructure or from distributed collectors to gather a detailed history of all network flow activity. QRadar supports industry-flow formats like Netflow, JFlow, SFlow and cflowd. All observed network flows are analyzed to build behavioral models that capture network behavior and to generate alerts when anomalous behavior is detected. QRadar learns the rate, volume and nature of network traffic to detect issues that affect service levels, and offers early detection that would otherwise go unnoticed (e.g. a mail virus that leverages the corporate SMTP server in the middle of the night).

This flow analysis enables QRadar passively monitors network activity and build real-time profiles of all network assets. It automatically measures risk exposure by augmenting these asset profiles with asset vulnerability, and activity data gathered from third-party vulnerability scanners. Furthermore, QRadar also maintains a stateful history of user identity on a per asset basis which is critical for integrating with NAC initiatives. As QRadar automatically builds these profiles from IPs appearing on the network, administrators have the ability to group and weight the importance of the assets and this weighting is used to determine a security event's priority when it occurs. This lets the QRadar administrator view any asset within the network and get a picture of that resource.

In the converging network and security infrastructure, the ability to relate what is reported from security products to what is observed on the network is critical. Not only is network traffic an important validation or contextual source for prioritizing security information, it is also vital in relating that information to the business assets that are deployed in a network. Once a business offense is detected, validated and fully understood, knowledge of the network provides more appropriate and timely response mechanisms.

QRadar Integration with TNC Access Control



Q1 Labs implements an interoperable access control facility based upon the Trusted Computing Group's Trusted Network Connect (TNC) Architecture. A review of the *TNC Architecture for Interoperability, Specification v1.1* is required to understand the content of this document.

The QRadar IMV leverages the user and host identity data collected within QRadar asset profile data to provide administrators with the means restrict or deny access to the network based upon user name or other credentials.

Based on the TNC architecture, when a client connection request is made:

1. The user initiates the access request via a TNC compliant client
2. The TNCC process loads all configured IMC libraries, in this case including the QRadar IMC
3. The IMC collects all the 'measurements' required and formats these into a message
4. The TNCC communicates the IMC messages to the TNCS which, in turn, passes them to the matching IMV
5. The QRadar IMV consults a Recommendation Service running on the QRadar console to obtain the basis of the recommendation
6. The QRadar IMV submits its recommendation to the TNCS

From the QRadar UI:

1. The QRadar admin right-clicks on an IP address and selects the Recommendation plugin.
2. The Admin creates deny or restrict access recommendations from the right-click plugin.
3. The recommendations are stored in the PostgresSQL database to be retrieved by the Recommendation Service.

The components of the TNC Architecture, including the function of the IMV and IMC are described in the *TNC Architecture for Interoperability, Specification v1.1* and other specification documents that can be found at http://www.trustedcomputinggroup.org/specs/TNC.

Example: QRadar integration with Juniper UAC Architecture

Through this integration, QRadar leverages the TNC open standards to communicate with the Juniper Networks UAC solution:

- The UAC solution offers a hardened policy management server that can push the UAC Agent to the endpoint (or gather information in agentless mode), to get user authentication, endpoint security state and device location. The UAC solution then combines that information with policy to provide per user, per session access enforced in the network.
- QRadar will provide user and machine based policy recommendations when it detects security incidents or anomalous network behavior occurring after trusted endpoints have been granted access to the network. With this post admission information, the Juniper Network UAC solution can then granularly quarantine an offending endpoint/user by controlling access to networks, resources and applications, only restoring access once the user returns to compliance.
- The information that QRadar leverages to signal Juniper Networks' UAC solution about threats detected within the network includes logs and alerts from heterogeneous host, application and security devices, including Juniper Networks' entire range of security technologies.

About Q1 Labs

Commanding a unique position at the nexus of security and networking, Q1 Labs is redefining network security management. Q1 Labs' flagship product, QRadar, integrates previously disparate network and security functions into one solution. This convergence ties the impact of security threats directly to specific business assets and services, reduces acquisition and operation costs and increases accuracy. Q1 Labs' installed customer base ranges from government agencies and financial institutions to universities and healthcare providers. Please visit http://www.q1labs.com/company/ or call (781) 250-5800 for more information.