Ribbon Analytics - NetProtect

Redefining the Real-time Communications Security Perimeter

Attacks on voice over IP (VoIP) traffic continues to increase and these new VoIP attacks are costing service providers and enterprises billions of dollars each year in toll fraud, theft of service, ransomware payments and more.

If you are managing a communications network, then you need to have a "zero-trust" strategy for both the external and internal aspects of your network. With VoIP, new doorways are being exposed to bad actors looking for easy access into your network. Therefore, the security stack must be re-architected to protect both data and voice across the entire network.

The market now demands a unified security perimeter that combines the capabilities of next generation firewalls with the capabilities of best-in-class session border controllers. Only by unifying the visibility and policy enforcement across voice and data domains can you ensure the most secure posture against new and existing attacks.

The Threat

Bad actors are constantly looking for ways to cause havoc either for monetary gains, to disrupt internal and external facing customer services, or just do reconnaissance into the entire corporate network. And, the rapid pace of growth for SIP-based real-time communications (RTC) has caught the attention of bad actors.

Bad actors are designing their attacks to bring down your communications infrastructure through means such as a telephony denial-of-service (TDOS) attack, voice phishing, registration floods, malicious endpoints, fraud, and SIP services password attacks. Bad actors can also exploit communication network vulnerabilities by eavesdropping on private communications or trying to access to a user's telephony account via registration hijacking so they can wreak havoc or just do reconnaissance in the entire corporate network.

Solution

To address the numerous types of RTC threats, Ribbon Analytics NetProtect application is the answer for your communication network that cannot be secured at any individual device or application layer. NetProtect coordinates RTC protection at the IP, application, and call layers which changes how RTC security is implemented.

With NetProtect, you can close the RTC security aperture against threats such as theft of service via RTP hijacking by identifying these threats in near real-time and then sharing dynamically created bad actor policies and enforcement methods back down into the entire network to prevent any further attacks. NetProtect also has a cooperative learning methodology with the other Protect RTC security and fraud-based applications by dynamically sharing its bad actor lists.

As shown in Figure 1 below, NetProtect redefines your RTC security protection by creating a security perimeter through network-wide detection, sharing and enforcement across all network elements such as Ribbon SBCs, 3rd Party SBCs, firewalls and other network devices. By linking the control plane messaging between platforms in real time, hacking efforts against your communications infrastructure are effectively blocked and the threats are mitigated.

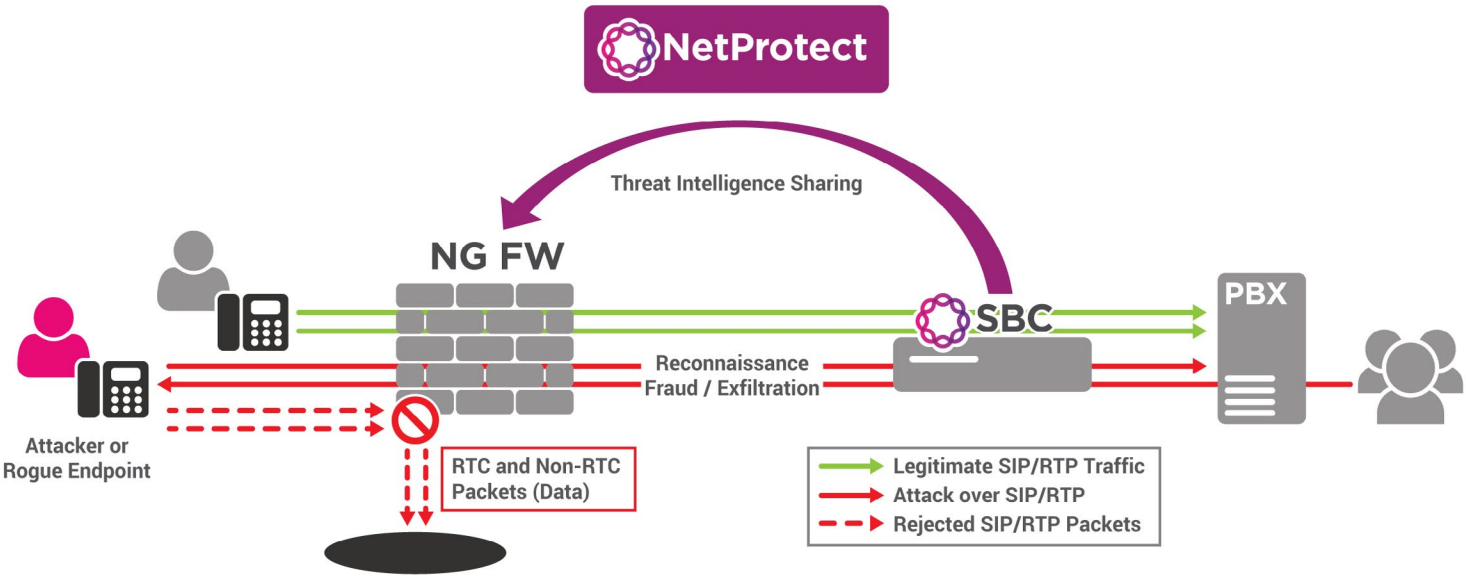

Figure 1. Threat Intelligence Sharing

Ribbon Protect Platform

NetProtect leverages Ribbon's Protect big data analytics platform to respond to real-time communications security and network quality incidents faster, more intelligently, and more efficiently.

The heart of the Protect platform is its UC anomaly detection and policy mitigation capability. The anomaly detection module collects and analyzes data across the entire communications network which is then made available to Ribbon Analytics applications. With customer-defined policy management functionality, detected anomalies generate alerts (e.g. SMS, email) and can be mitigated with actions to the appropriate network elements in real-time.

www.rbbn.com