Redefining the Enterprise Security Perimeter

Connecting SBCs and NGFWs for unprecedented security protection

Attacks on enterprise unified communications (UC) traffic continue to increase and these VoIP attacks are costing service providers and enterprises billions of dollars each year in toll fraud, theft of service, ransomware and more. Most recently, black hats are targeting SIP-based infrastructure for data exfiltration attacks, the most lucrative, devastating, and prevalent threat. If that wasn't enough, enterprises continue migrating to SD-WAN with underlying internet broadband-based architectures, making the job of securing the enterprise perimeter even more challenging.

The market demands a new unified enterprise security perimeter that combines the capabilities of next generation firewalls (NGFWs) with best-in-class session border controllers (SBCs). Only by unifying visibility and control across voice and data domains can enterprises ensure the most secure possible posture against new and existing attacks.

The Threat

Bad actors are constantly looking for ways to cause havoc in enterprises, either for monetary gains or to disrupt internal- and external-facing customer services. SIP-based UC growth has caught the attention of hackers, and now exposes additional security threats to the enterprise. These attacks may be intended to bring a communications system down, by executing a telephony denial-of-service (TDoS) attack or a registration flood. These attacks could be economics-based, using techniques such as voice phising, theft of service, fraud, and data exfiltration. Data exfiltration attacks are designed to steal confidential information via exfiltration which passes stolen corporate data through a normal SIP call. Or even consider how bad actors can also exploit UC vulnerabilities to eavesdrop on private communications.

Attacks on UC are real and growing. To address this threat, Palo Alto Networks and Ribbon are working together to connect their NGFW and SBCs to create a new, unified enterprise security perimeter. By linking the control plane messaging between both platforms in real-time, new and existing hacking efforts against enterprise UC infrastructures will be effectively blocked.

Today, firewalls and SBCs operate independently and do not share insights on potential threats (see figure 1). Most enterprises have shifted their UC traffic to SIP services from their service provider to help cut costs and enable flexible services. Typically, service provider SIP trunking services terminate their SIP traffic on an SBC using a dedicated data circuit. However, over-the-top (OTT) communication providers (UCaaS providers) will terminate their SIP traffic via the internet directly to a firewall.

These UC infrastructures are SIP-based and vulnerable because they:

1. Lack an SBC at the edge necessary to block malicious SIP traffic (37% of enterprises that utilize SIP trunks do not have SBCs).
2. Use a firewall instead of an SBC for SIP traffic. In fact, most enterprises are turning off the SIP-ALG (application layer gateway) in NGFWs, since SIP-ALGs can cause problems for voice redirect calls.
3. Have no way of linking SBCs and NGFWs to block new data exfiltration attempts that use phishing attacks to gain access and exfiltrate enterprise data over SIP and UDP.
4. Increasingly use direct internet access for branch access (SD-WAN), thereby creating a broader enterprise perimeter to secure.

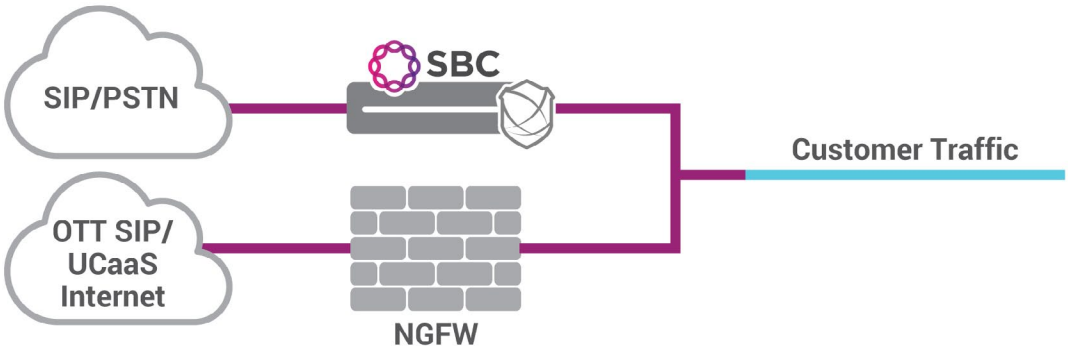

Figure 1: NGFW and SBC operating independently to secure all collaboration traffic.

Solution

To address these vulnerabilities, Ribbon Analytics' NetProtect application is the answer.

NetProtect coordinates Unified Communications protection at the IP, application, and call layers which fundamentally changes how security is implemented to provide a unified security perimeter. With NetProtect, you are able close the UC security aperture by identifying these threats in near real-time and then dynamically sharing bad actor policies and enforcement methods into the entire network to prevent any further attacks. NetProtect is fully virtualized, so an enterprise team can deploy it on a variety of platforms, including public clouds.

As shown in Figure 2 below, NetProtect enables a much wider security perimeter through network-wide detection, sharing and enforcement across all network elements, such as Ribbon SBCs, 3rd Party SBCs, firewalls or 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

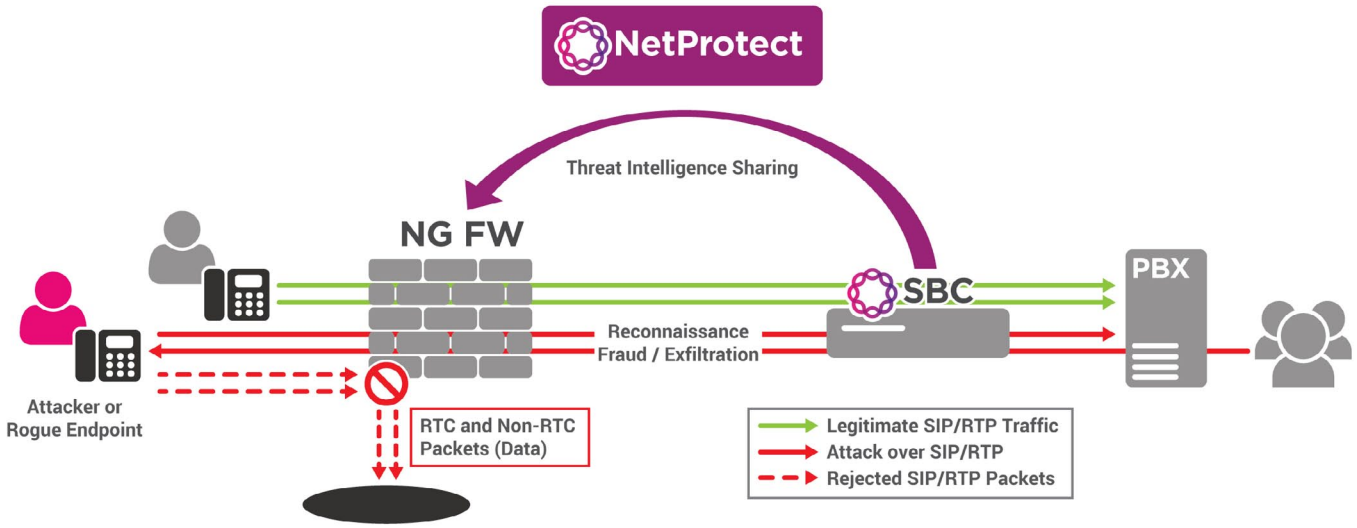

Figure 2: Threat Intelligence Sharing

Ribbon Analytics Protect Platform

NetProtect leverages Ribbon Analytics' Protect 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 big data engine that provides anomaly detection and policy mitigation capabilities. The anomaly detection module collects and analyzes data across the entire communications network and then makes it available to Ribbon Analytics applications, like NetProtect.

With customer-defined policy management functionality, alerts are raised on detected anomalies and can be manually or automatically mitigated with appropriate actions.

With this innovative solution, the Ribbon SBC and next generation firewalls (NGFW), such as those from Palo Alto Networks, act in series rather than in parallel to jointly leverage their optimized security capabilities. This effectively raises the trust level of UC in the network, and raises the overall security posture of the enterprise. By linking the two platforms at the control plane level, the NGFW and SBC now share important threat intelligence and work together to block current and potential new UC-based attacks.

Ribbon NetProtect will share both black-list and white-list information with the Ribbon SBC and the Palo Alto Networks NGFW. This enables the platforms to work in tandem to 1) identify that the correct IP address pairs are allowed within a SIP trunk or 2) block bad actors when identified. If the SBC detects bad actor behavior from a UC device, it can signal the NGFW to act and block access, or the NGFW will inherently block access. The reverse is also true, in that the SBC can signal that certain end points are now white-listed and the NGFW can remove them from the black-list. **The benefit is that bad behavior can be identified and acted upon per IP address in near real time as well as triggering the NGFW to block bad actors across other applications. This unifies the enterprise data and UC security perimeters.**

The Ribbon SBC and the Palo Alto Networks NGFW platforms are able to work in unison to allow session attribute provisioning. This means UC traffic is allowed on a white-list basis only (and not on a black-list exception basis). Based on input from NetProtect, the Palo Alto Networks NGFW opens and closes media flows on a per call/per flow basis, which eliminates nearly all possible attack vectors. In other words, the UC security posture shifts from "admit and verify" to "allow trusted flows only." **The benefit is that the enterprise can now implement a new level of security that is provisioned automatically and adapts in real-time.**

About Palo Alto Networks

Palo Alto Networks is the next-generation security company maintaining trust in the digital age by helping tens of thousands of organizations worldwide prevent cyber breaches. Our innovative security platform with game-changing technology natively brings network, cloud and endpoint security into a common architecture. By doing this, we safely enable applications, users, and content; deliver visibility, automatio, and control; and detect and prevent threats at every stage of the attack lifecycle, so organizations can securely and efficiently move their businesses forward.

About Ribbon Communications

Ribbon Communications (Nasdaq: RBBN) delivers communications software, IP and optical networking solutions to service providers, enterprises and critical infrastructure sectors globally. We engage deeply with our customers, helping them modernize their networks for improved competitive positioning and business outcomes in today's smart, always-on and data-hungry world. Our innovative, end-to-end solutions portfolio delivers unparalleled scale, performance, and agility, including core to edge software-centric solutions, cloud-native offers, leading-edge security and analytics tools, along with IP and optical networking solutions for 5G. We maintain a keen focus on our commitments to Environmental, Social and Governance (ESG) matters, offering an annual Sustainability Report to our stakeholders. To learn more about Ribbon visit rbbn.com.

Contact Us Contact us to learn more about Ribbon solutions.

Microsoft Partner
Gold Communications

Voice
Unified Communications
Business Productivity Solutions
Midmarket Solution Provider