Technical Disclosure Commons

Defensive Publications Series

October 2019

ROBO-CALLING PREVENTION WITH SOFTWARE-DEFINED NETWORKING IN A WIDE AREA NETWORK POLICY FOR UNIFIED COMMUNICATION

Balaji Sundararajan

Anand Oswal

Vivek Agarwal

Rong Wang

Palak Desai

ROBO-CALLING PREVENTION WITH SOFTWARE-DEFINED NETWORKING IN A WIDE AREA NETWORK POLICY FOR UNIFIED COMMUNICATION

AUTHORS:
Balaji Sundararajan
Anand Oswal
Vivek Agarwal
Rong Wang
Palak Desai

ABSTRACT

Techniques are described herein for blocking robo-calls, spam calls, and telemarketing calls, which are becoming an industry menace. Such calls are blocked by tightly integrating a Software-Defined Networking in a Wide Area Network (SDWAN) controller with a Do Not Call registry. Analytics are used to analyze traffic call patterns, security insights are leveraged such as known malicious Internet Protocol (IP) and domain addresses, and a Call Barring feature may also be applied. This information may be pushed to edge devices to ensure robo-calls do not terminate on SDWAN-led voice endpoints.

DETAILED DESCRIPTION

A robo-call is a phone call that, when answered, plays a recorded message instead of a live person. Scammers make illegal calls from anywhere in the world, and hide from law enforcement by displaying fake caller Identification (ID) information. Scammers often leave voice messages to prompt users to call back, which can lead to expensive phone calls. In addition, telemarketers frequently spam employees in an enterprise, impacting productivity and potentially risking network security. Described herein are solutions to address these problems.

Today, unified communication (e.g., unified voice communication) is implemented at enterprise branches. There is a need to integrate this tightly with Software-Defined Networking in a Wide Area Network (SDWAN) so that call control (e.g., call setup, call tear down, etc.) over existing methods can be established in the best possible SDWAN path. This prevents robo-calls and telemarketing calls by linking the system to a Do Not Call registry.

When a new call arrives, the system performs a look up in the Do Not Call registry to determine whether the potential call is a possible spam or robo-call. A smart policy may be used to distribute the call to the enterprise sites, which host unified communication setup and block the incoming phone calls.

Telemarketing calls may also be identified using SDWAN analytics. The SDWAN control policy may be used to prevent spam calls by distributing a Call Barring feature to all branches having edge and/or unified communication endpoints in the network.

Furthermore, for calls made from fake but legitimate numbers, the solution may use machine learning to map caller ID with suspicious Internet Protocol (IP) and domain addresses to a blocked number list. This solution may be useful for corporate companies to filter calls based on caller ID, the Do Not Call registry, and call patterns indicating spam. This blocked entry may be redistributed to all edge routers. This may help enterprises protect employee privacy and prevent illegal calling into the enterprise via smart SDWAN policies.

Thus, spam control may be provided for enterprise networks. SDWAN enables control of unified communication, call admission, spam call detection, sharing of spam call details across enterprises, and spam and robo-calling prevention.

Figure 1 below illustrates an example call control architecture. At step 1, spam calls are learned from sites and the do not call registry list on vManage. At step 2, a vSmart controller redistributes IP information to Software-Defined Wide Area Network (SDWAN) devices. At step 3, the vSmart policy is registered with the SDWAN devices. At step 4, the SDWAN entries are programmed into Ternary Content-Addressable Memory (TCAM) on the devices. At step 5, new traffic arrives at the branch, and the branch determines whether the new traffic is associated with a spam call. If not, the branch queries via vSmart and vManage from external sources to check the origin of calls. If found to be a spam call, this information is fed back to the vSmart controller.

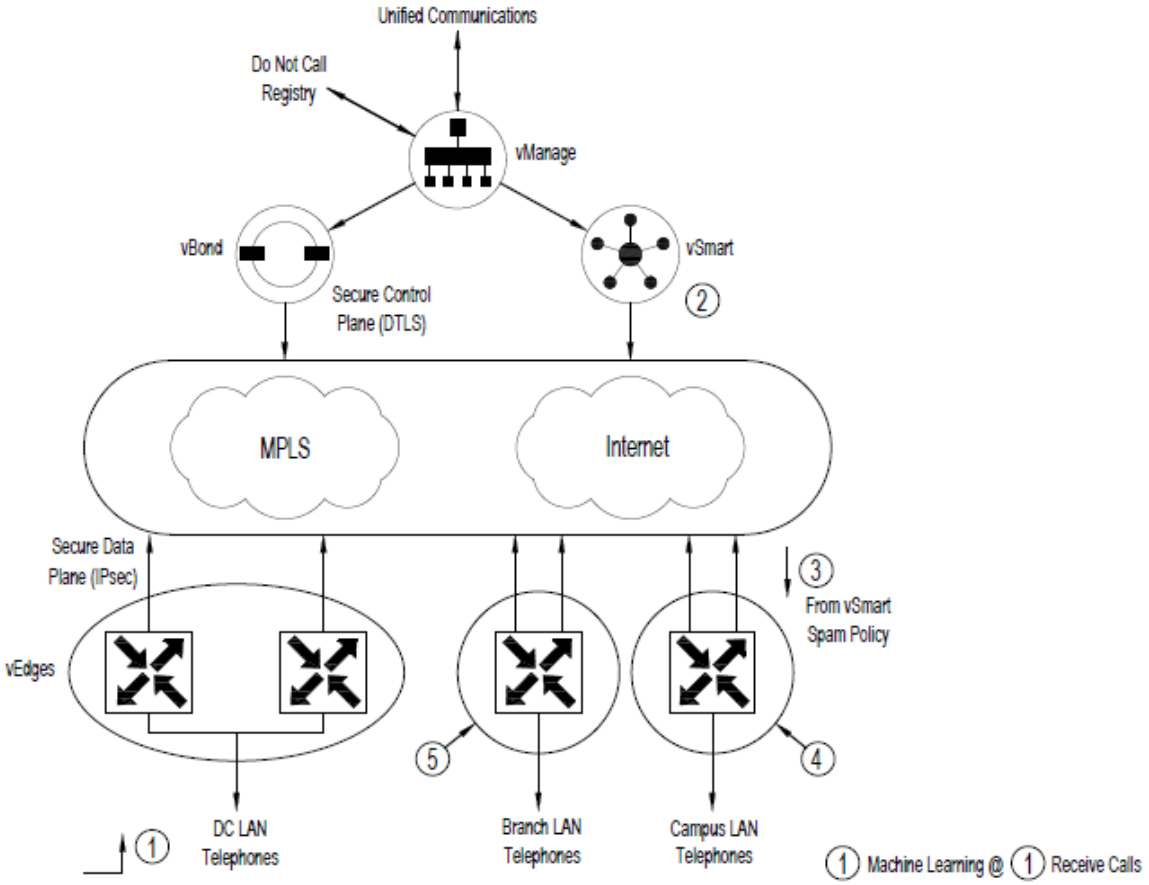
Unified Communications
Do Not Call Registry
vManage
vBond
vSmart
Secure Control Plane (DTLS)
2
MPLS
Internet
Secure Data Plane (IPsec)
3
From vSmart Spam Policy
vEdges
5
4
1
DC LAN Telephones
Branch LAN Telephones
Campus LAN Telephones
1 Machine Learning @ 1 Receive Calls

Figure 1

Figure 2 below illustrates another example call control architecture.

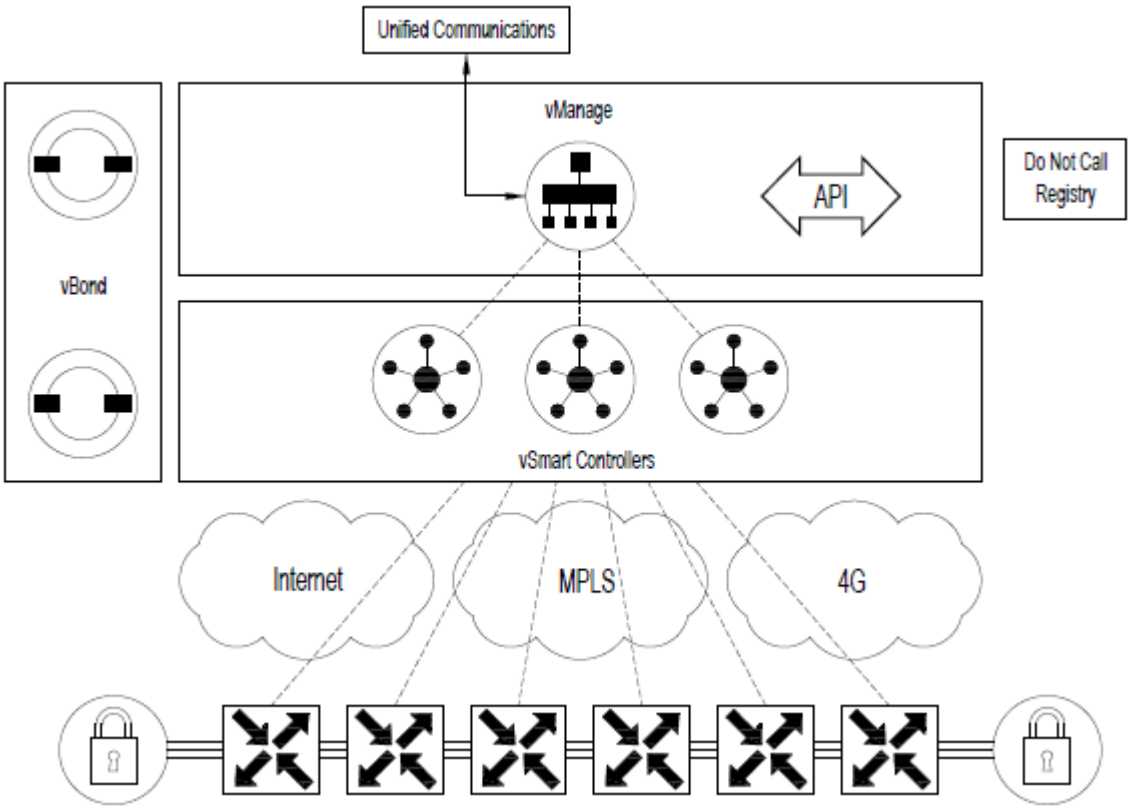

Figure 2

In summary, techniques are described herein for blocking robo-calls, spam calls, and telemarketing calls, which are becoming an industry menace. Such calls are blocked by tightly integrating a SDWAN controller with a Do Not Call registry. Analytics are used to analyze traffic call patterns, security insights are leveraged such as known malicious IP and domain addresses, and a Call Barring feature may also be applied. This information may be pushed to edge devices to ensure robo-calls do not terminate on SDWAN-led voice endpoints.