ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 85 – 89 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

Access policy and security of Multiple Entry Points with VPNs

A.Santhoshi[#1], G.Swathi[#2], K.Ashwini[#3]

Asst.professor[#1,] Department of Computer Science and Engineering, Malla Reddy Institute Of Engineering and Technology, Hyderabad, India.
Student[#2,] Department of Computer Science and Engineering, Malla Reddy Institute Of Engineering and Technology, Hyderabad, India.
Student[#3,] Department of Computer Science and Engineering, Malla Reddy Institute Of Engineering and Technology, Hyderabad, India.

[#1]angursanthoshi@gmail.com
[#2]gaddamswathi760@gmail.com
[#3]ashwini529.reddy@gmail.com

Abstract-The current event processing system worked on the consolidation of one hop to other single hop[1].The present system having lack of security in multi-hop processing[2]. This is the problem in large scale distribution applications in multiple security domains. This paper presents an approach that allows the load sharing, high availability and security in single source to multiple destinations by using multiple entry point(MEP) of virtual private network(VPN) .It addressed the methods are explicit MEP and implicit MEP.Here the implementation of multiple entry point with explicit MEP and multi-hop network is secured by the virtual private networks(VPNs)[3].

Keywords–
VPN, Multiple Entry Point (MEP), Load Sharing, High availability.

Introduction

Multiple Entry Point (MEP) is a feature that provides a high availability and load sharing solution for VPN connections [4]. A Security Gateway on which the VPN module is installed provides a single point of entry to the internal network. It is the Security Gateway that makes the internal network "available" to remote machines. If a Security Gateway should become unavailable, the internal network too, is no longer available. A MEPed environment has two or more Security Gateways both protecting and enabling access to the same VPN domain, providing peer Security Gateways with uninterrupted access[5]

.

Implementation

MEP is implemented via a proprietary *Probing Protocol* (PP) that sends special UDP RDP packets to port 259 to discover whether an IP is reachable. This protocol is proprietary to Check Point and does not conform to RDP as specified in RFC 908/1151

The peer continuously probes or polls all MEPed Security Gateways in order to discover which of the Security Gateways are "up", and chooses a Security Gateway according to the configured selection mechanism[6]. Since RDP packets are constantly being sent, the status of all Security Gateways is known and updated when changes occur. As a result, all Security Gateways that are "up" are known.

There are two available methods to implement MEP:

- **Explicit MEP -** Only Star communities with more than one central Security Gateway can enable explicit MEP, providing multiple entry points to the network behind the Security Gateways. When available, Explicit MEP is the recommended method[7].
- **Implicit MEP -** Implicit MEP is supported in all scenarios where fully or partially overlapping encryption domains exist or where primary backup security gateways are configured[8]. When upgrading from a version prior to NGX (R60) where Implicit MEP was already configured, the settings previously configured will remain.

Explicit MEP

In a site to site Star VPN community, explicit MEP is configured via the community object. When MEP is enabled, the satellites consider the "unified" VPN domain of all the Security Gateways as the VPN domain for each Security Gateway. This unified VPN domain is considered the VPN domain of each Security Gateway:

M1 and M2 (for which MEP has been enabled) and three satellite Security Gateways — S1, S2, and S3. When S2 opens a connection with host-1 (which is behind M1 and M2), the session will be initiated through either M1 or M2. Priority amongst the MEP Security Gateways is determined by the MEP entry point selection mechanism.

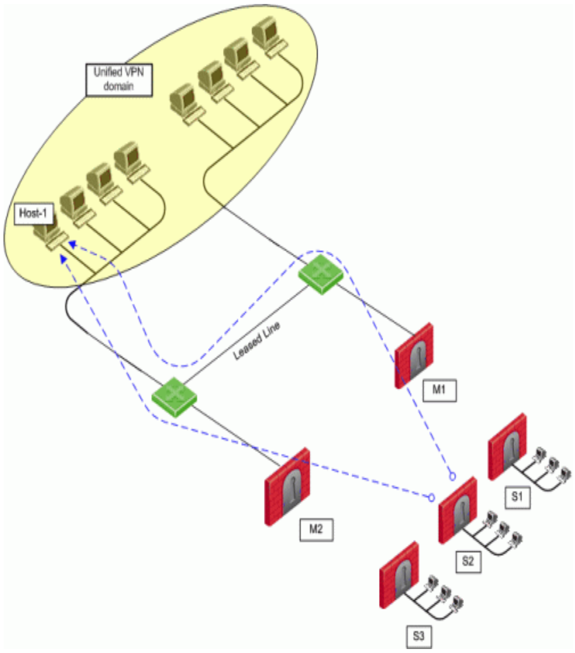

Figure 1: a Star VPN community has two central Security Gateways

If M2 is the selected entry point and becomes unavailable, the connection to host-1 fails over to M1. Returning packets will be rerouted using RIM or IP Pool NAT. For more information about returning packets,

There are four methods used to choose which of the Security Gateways will be used as the entry point for any given connection:

- Select the closest Security Gateway to source (First to respond)
- Select the closest Security Gateway to destination (By VPN domain)
- Random Selection (for Load distribution)
- Manually set priority list (MEP rules)

MEP Selection Methods

- **First to Respond**, in which the first Security Gateway to reply to the peer Security Gateway is chosen. An organization would choose this option if, for example, the organization has two Security Gateways in a MEPed configuration - one in London, the other in New York. It makes sense for peers located in England to try the London Security Gateway first and the NY Security Gateway second. Being geographically closer to the peers in England, the London Security Gateway will be the first to respond, and becomes the entry point to the internal network.
- **VPN Domain,** is when the destination IP belongs to a particular VPN domain, the Security Gateway of that domain becomes the chosen entry point. This Security Gateway becomes the primary Security Gateway while other Security Gateways in the MEP configuration become its backup Security Gateways.

Random Selection, in which the remote peer randomly selects a Security Gateway with which to open a VPN connection. For each IP source/destination address pair, a new Security Gateway is randomly selected. An organization might have a number of machines with equal performance abilities. In this case, it makes sense to enable load distribution. The machines are used in a random and equal way.

- **Manually set priority list,** Security Gateway priorities can be set manually for the entire community or for individual satellite Security Gateways.
- **MEP Selection Methods**
- **First to Respond**, in which the first Security Gateway to reply to the peer Security Gateway is chosen. An organization would choose this option if, for example, the organization has two Security Gateways in a MEPed configuration - one in London, the other in New York. It makes sense for peers located in England to try the London Security Gateway first and the NY Security Gateway second. Being geographically closer to the peers in England, the London Security Gateway will be the first to

respond, and becomes the entry point to the internal network.

- **VPN Domain,** is when the destination IP belongs to a particular VPN domain, the Security Gateway of that domain becomes the chosen entry point. This Security Gateway becomes the primary Security Gateway while other Security Gateways in the MEP configuration become its backup Security Gateways.
- **Random Selection**, in which the remote peer randomly selects a Security Gateway with which to open a VPN connection. For each IP source/destination address pair, a new Security Gateway is randomly selected. An organization might have a number of machines with equal performance abilities. In this case, it makes sense to enable load distribution. The machines are used in a random and equal way.
- **Manually set priority list,** Security Gateway priorities can be set manually for the entire community or for individual satellite Security Gateways.

First to Respond

When there is no primary Security Gateway, all Security Gateways share "equal priority". When all Security Gateways share equal priority:

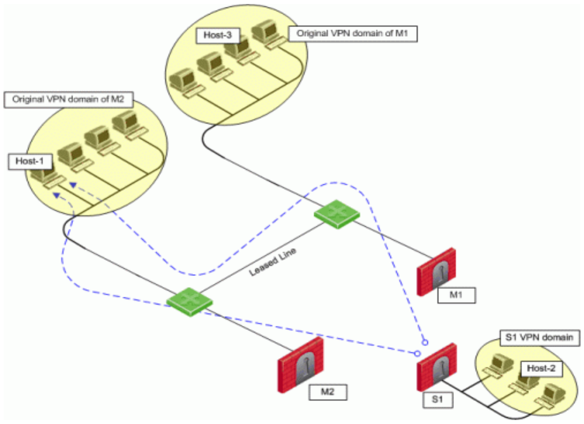

Figure 2: the VPN Star community has two central MEPed Security Gateways (M1 and M2, each of which *have their own VPN domains*)and remote satellite S1.

- Remote peers send RDP packets to all the Security Gateways in the MEP configuration.

- The first Security Gateway to respond to the probing RDP packets gets chosen as the entry point to network. The idea behind *first to respond* is proximity. The Security Gateway which is "closer" to the remote peer responds first.

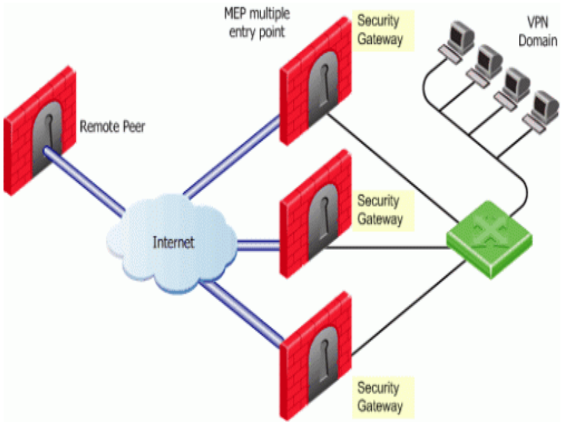

Figure 3:Primary security gateways

A VPN tunnel is opened with the first to respond. All subsequent connections pass through the chosen Security Gateway.
If the Security Gateway ceases to respond, a new Security Gateway is chosen.

By VPN Domain

Prior to enabling MEP, each IP address belonged to a specific VPN domain. Using *By VPN Domain*, the Security Gateway of that domain becomes the chosen entry point.

Host-2 (in the VPN domain of satellite S1 initiates a connection with host-1. The connection can be directed through either M1 or M2. However, host-1 is within M2's original VPN domain. For this reason, M2 is considered the Security Gateway "closest" to the destination IP Address. M2 is therefore considered the primary Security Gateway and M1 the backup Security Gateway for Host-1. If there were additional Security Gateways in the center, these Security Gateways would also be considered as backup Security Gateways for M2.

If the VPN domains have fully or partially overlapping encryption domains, then more than one Security Gateway will be chosen as the "closest" entry point to the network. As a result, more than one Security Gateway will be considered as "primary." When there are more than one primary or backup Security Gateways available, the Security Gateway is selected using an additional selection mechanism. This advanced selection mechanism can be either First to Respond

- Random Selection (for load distribution)
- For return packets you can use RIM on the center Security Gateways. If RIM is also enabled, set a metric with a lower priority value for the leased line than the VPN tunnel. The satellite S1 might simultaneously have more than one VPN tunnel open with the MEPed Security Gateways, for example M2 as the chosen entry point for host-1 and M1 as the chosen entry point for host-3. While both M1 and M2 will publish routes to host-1 and host-3, the lower priority metric will ensure the leased line is used only when one of the Security Gateways goes down.
- **Random Selection**
- Using this method, a different Security Gateway is randomly selected as an entry point for incoming traffic. Evenly distributing the incoming traffic through all the available Security Gateways can help prevent one Security Gateway from becoming overwhelmed with too much incoming traffic.
- The Security Gateways are probed with RDP packets, as in all other MEP configurations, to create a list of responding Security Gateways. A Security Gateway is randomly chosen from the list of responding Security Gateways. If a Security Gateway stops responding, another Security Gateway is (randomly) chosen.
- A new Security Gateway is randomly selected for every source/destination IP pair. While the source and destination IP's remain the same, the connection continues through the chosen Security Gateway.
- *In such a configuration, RIM is not supported*. IP Pool NAT must be enabled to ensure return packets are correctly routed through the chosen Security Gateway.
- **Manually Set Priority List**
- The Security Gateway that will be chosen (from the central Security Gateways in the star community) as the entry point to the core network can be controlled by manually setting a priority per source Security Gateway. Each priority constitutes a MEP Rule:

- In Satellite S1 can be configured to try the Security Gateways in the following order: M1, M2, M3, giving the highest priority to M1, and the lowest priority to M3. Satellite S2 can be configured to try the Security Gateways in the following order: M2, M3 (but not to try M1).

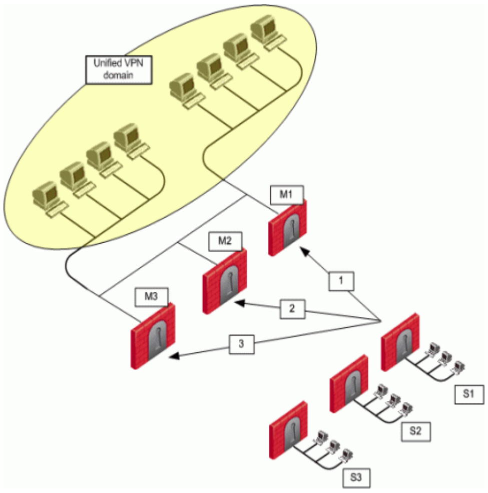

Figure 4: Three MEP members (M1, M2, M3) provide entry points to the network for three satellite Security Gateways (S1, S2, S3).

- Each of these priorities constitutes a MEP rule in the MEP manual priority list window:

Advanced Settings

In some instances, more than one Security Gateway is available in the center with no obvious priority between them. Advanced options are used to decide which Security Gateway is chosen: *First to Respond*, or *Random Selection*. (Choose Random selection to enable load balancing between the Security Gateways.)

- When "manually set priority list" is the MEP selection mechanism, *RIM is supported.* RIM can be configured with "manually set priority list" because the "random selection" mechanism available on the Advanced button is different from the random selection mechanism used for MEP.For the "random selection" mechanism employed for MEP, a different Security Gateway is selected for each IP source/destination pair. For the random selection mechanism available from the Advanced button, a single MEP entry point is randomly selected and then used for all connections, and does not change according to source/destination pair. Load distribution is therefore achieved since every satellite Security Gateway is randomly assigned a Security

Gateway as its entry point. This makes it possible to enable RIM at the same time.

- Whether the resolved Security Gateway is responding.

Conclusion

This paper addressed the inheritance and consolidation of access policies in heterogeneous VPN systems. We presented an implementation of our approach based on explicit MEP. Future work will concentrate on enhancing the implicit MEP methods to increase the more security and high load sharing.

References

1. Access policy consolidation for event processing system Bjorn Schilling,Boris Koldehofe,Kurt Rothermel and UmaKishore Ramachandran.
2. S.Rizou,F.Durr and K.Rothermel,"providing qos guarentees in large scale operator networks"in High Performance Computing and Comunications.
3. Mason, Andrew G. *Cisco Secure Virtual Private Network*. Cisco Press, 2002, p. 7
4. Microsoft TechNet. "Virtual private Networking"
5. Cisco Systems, et al..*Internet working Technologies Handbook, Third Edition*. Cisco Press, 2000, p. 232.
6. Lewis, Mark. *Comparing, Designing. And Deploying VPNs*. Cisco Press, 20069, p.
7. International Engineering Consortium. *Digital Subscriber Line 2001*. Intl. Engineering Consortium, 2001, p. 40.www.iec.org
8. Technet Lab. IPV6 trafic over VPN connections.
9. VPN Consortium "VPN TECHNOLOGIES".
10. RFC 6434 "IPv6 Node Requirements", E. Jankiewicz, J. Loughney, T. Narten (December 2011)
11. "openconnect".Retrieved 2013-04-08. "Open Connect is a client for Cisco's Any Connect SSL VPN [...]
12. B. Schilling, B. Koldehofe, and K. Rothermel, "Efficient and distributed rule placement in heavy constraint-driven event systems," in Proc. of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC) , 2011, pp. 355–364.
13. Book:Endpoint security VPN administration guide-77

About Authors:

1. A.SANTHOSHI has received her B.Tech degree fromVREC(Jawaharlal Nehru Technology University, hyderabad and M.Tech from JBIET(Jawaharlal Nehru Technology University), Hyderabad.Now working as an Asst.professor in MallaReddy Institute of Engineering & Technology.

2. G.SWATHI doing her B.Tech in MallaReddy Institute of Engineering & Technology.

3.K.ASWINI doing her B.Tech in MallaReddy Institute of Engineering & Technology.