Network Working Group
Internet Draft
Intended status : Informational
Expires : December 15, 2011

Michael Ko
Edward Wang
Huawei Symantec
June 15, 2011

# Problem Statement for Setting Up Dynamic Virtual Network
# draft-ko-dvn-problem-statement-00.txt

Abstract

This document examines the problems and challenges associated with the process of setting up secure virtual network connections among authorized network nodes. The network nodes can be located anywhere in a private or public network, directly connected or behind one or more levels of NAT. Setting up a secure virtual network in this environment entails the resolution of various issues such as authentication, peer discovery, virtual network address management, and connection parameters determination.



Table of Contents

## 1 Introduction

The pervasiveness and the ubiquity of the Internet have empowered mobile users, bringing it closer to reality for anyone to achieve the goal of being able to work anywhere, anytime, and using any device. The user's computer may only contain just a minimal operating system with a web browser to serve as little more than a display terminal for processes occurring on a network of computers far away. Therefore, being able to setup a connection with any authorized network nodes containing the needed resources on demand will further increase the flexibility for the user, allowing him/her to pick and choose the appropriate resources based on different criteria for the task at hand. These network nodes containing the needed resources may reside inside the local network, or externally at an internet connected datacenter.

A user may need to set up a secure connection with an authorized network node for data backup and archiving purposes. This allows a user that stores his/her data at one facility (such as a cloud storage facility) to backup and archive his/her data at a different facility (such as a different cloud storage facility) in order to avoid suffering irrecoverable data loss in a catastrophic situation.

A user may want to set up a secure connection with a remote authorized network node for data mirroring purposes. This allows a mobile user to maintain remote copies of the data at different locations. Then depending on his/her current location, he/she can select the nearest network node containing a replica of his/her data in order to lower the access latency.

In some anti-DDoS (distributed denial of service) solutions, the network node running the operation of the anti-DDoS solution is responsible for formulating the detection and cleaning policies based on user defined requirements. The network node needs to set up secure connections with the network nodes responsible for DDoS detection and the network nodes responsible for cleaning in order to deliver the policies for execution. In turn, each network node containing the DDoS detectors identifies and detects DDoS traffic,

and periodically sets up a secure connection with the network node running the operation to return the detection results in order for the cleaning policies to be updated based on the detection results. Similarly, each network node acting as a cleaning agent filters DDoS traffic and isolates threats, and periodically sets up a secure connection with the network node running the anti-DDoS solution in order to receive updated cleaning policies.

These and other examples point to the need for setting up virtual network connections with authorized network nodes anywhere in the Internet in a secure manner for various reasons.

## 2 Problems in Establishing Network Connections

Setting up a network connection with authorized network nodes entails challenges related to connectivity, security, and management in the process of establishing and maintaining a virtual network connecting the two network nodes.

### 2.1 Connectivity Problems

The first consideration for a user in setting up a connection with an authorized network node is the ability to create an end-to-end connection between the two nodes. Ideally any node connected to the Internet should be able to establish addressing and create direct end-to-end connection with the other network node regardless of its topological location and Internet Protocol technology (IPv4/v6). In reality, a network node can be located anywhere in a private or public network, directly connected or behind one or more levels of NAT. In addition, it is not uncommon for a node to have a dynamic IP address on its physical or virtual interfaces. Furthermore, the status of a node being online or offline is dynamic. For a mobile user, even the physical location of a node is also dynamic.

Due to the dynamic nature of these virtual networks, automated discovery is an important requirement for the user to set up a secure network connection with an authorized network node. The IETF standard known as the Service Location Protocol [SLP] allows computers and other devices to find services in a local area network. In larger networks, one or more "directory agents" are used in SLP. Service agents send register messages containing all the services they advertise to the "directory agents". User agents issue service requests to the "directory agent", specifying the characteristics of the services they require. To provision services to users, a network administrator can assign a scope string to each and every user agent in order to limit the user agent to discover only that particular grouping of services. As currently defined,

the "directory agent" merely functions as a cache and does not have the authority to set the scopes for the user agents.

In some cases it is not possible to establish a direct end-to-end connection especially when both parties are located behind NATs. The IETF standard known as Traversal Using Relays around NAT [TURN] allows a host behind a NAT to use the services of an intermediate node that acts as a communication relay in order to exchange packets with its peers. A client using TURN must have some way to communicate the relayed transport address to its peers, and to learn each peer's IP address and port (more precisely, each peer's server-reflexive transport address). This can be done using a special-purpose "introduction" or "rendezvous" protocol (see [RFC5128]), but it does require the use of a publicly addressable "rendezvous server".

The Internet Storage Name Service [iSNS] protocol facilitates the automated discovery, management, and scalable configuration of Internet Small Computer Systems Interface [iSCSI] devices on a TCP/IP network. iSNS allows the administrator to go beyond a simple device-by-device management model, where each storage device is manually and individually configured with its own list of known initiators and targets. Using iSNS, each storage device subordinates its discovery and management responsibilities to an "iSNS server". The "iSNS server" serves as the consolidated configuration point through which management stations can configure and manage the entire storage network. With the iSNS protocol supporting the interaction between "iSNS servers" and iSNS clients, iSNS provides the intelligent storage discovery and management services needed. However, iSNS is intended to emulate Fibre Channel fabric services and to manage both iSCSI and Fibre Channel devices, and is therefore not suitable for use outside of the storage area network.

The iSNS model points to the desirability of subordinating the network nodes to a consolidated configuration point for scalability reasons. This allows the network administrator to use the consolidated configuration point through which management stations can configure and manage the virtual network, instead of the simple node-by-node management model, where each network node is manually and individually configured with its own list of authorized network nodes. The consolidated configuration point, acting as a central repository, can facilitate the automated discovery problem since it contains the necessary parameters for network nodes to discover and construct virtual networks with other authorized network nodes. Certain parameters can be pre-configured by the network administrator while others can be dynamically provided by the

network nodes. The parameters may contain the topology of the overlay network (e.g., hub-and-spokes or hub), the function type of specific network nodes (e.g., router or host), the tunneling method (e.g., IPsec), the routing protocols (e.g., OSPF), or routing lookup method (e.g., DNS lookup), the dynamic physical and virtual IP addresses of the network nodes, etc. For NAT traversal, the central repository can also serve as the rendezvous server. Existing standards that use central repositories such as the SLP "directory agent", the "iSNS server", etc., provide some but not all of the functionalities needed.

Existing methodologies can be used by network nodes to discover the central repository, such as pre-configuring the domain name or address of the central repository in the network nodes, or provisioning via Dynamic Host Configuration Protocol [DHCP] or Domain Name System [DNS] lookup, etc. When a network node wishes to join the virtual network, either seeking to connect to other network nodes, or allowing others to connect to it, it contacts a central repository to login to the virtual network in order to register and activate its presence in the virtual network. After successful login, a network node may register additional information (e.g., its dynamic IP address) with the central repository so that the information can be shared with other authorized network nodes. The central repository in turn provides the network node with the necessary information needed to establish a connection with other network nodes. Through the central repository, a network node should be able to determine other network nodes that it is authorized to access, the online status of other network nodes, parameters needed to establish a connection, etc.

## 2.2 Security Problems

The second consideration in setting up a connection with authorized network nodes is security. Ideally any node with the same security/application strategy can form a dynamic virtual network free of the restrictions of the physical network, and network Security Assurance solutions should not be dependent on network topology. The dynamic virtual network should provide unified security services for trusted network construction, authentication and access control, data confidentiality and data integrity, and non-repudiation.

In a datacenter, there are identifiable boundaries to an enclave (the collection of local computing devices that are governed by a single security policy). This facilitates the defense of the enclave boundary by focusing on effective control and monitoring of data flow into and out of the enclave. Effective control measures

include firewalls, guards, Virtual Private Networks [VPN], and identification and authentication /access control for remote users. Effective monitoring mechanisms include network-based Intrusion Detection System (IDS), vulnerability scanners, and virus detectors located on the LAN (see [IATF].)

On the Internet, critical systems are exposed, and physical isolation can no longer be relied upon to enforce security. Instead, each network node must be treated as a separate enclave and be protected as such. There is a need for client authentication, peer discovery, virtual network address management, etc. in order to enable a user to setup a secure connection.

Various IETF standards on security such as IP Security [IPSEC], Transport Layer Security [TLS], Secure Shell [SSH], Public-Key Cryptography Standards [PKCS], etc, provide the needed framework for network nodes to create security tunnels to satisfy the security requirement. But to create a security tunnel during connection establishment, a network node may need to have access to certificate fingerprint (see [RFC4572]), generated keys and security strategy, etc. These can be facilitated by having a central repository in the virtual network responsible for disseminating the required information. A central repository is also needed to handle the authentication, authorization and accounting for a network node after the network node presents its identity and credentials to the central repository upon login. This means that the network node and the central repository may share a pre-configured or automatically established security association to prevent unauthorized access.

## 2.3 Management Problems

The third consideration in setting up a connection with authorized network nodes is on management and control. The following is a list of some of the critical management tasks that are required for setting up a connection with an authorized network node:

1. Discover the network nodes that a user is authorized to access are currently online and active.

2. Discover the functional attributes associated with these authorized network nodes.

3. Discover the location of the authorized network nodes.

4. Determine if accessing the network node requires going through a relay (e.g., TURN). Discover the location of the relay if it is needed.

5. Determine the parameters needed to set up a secure connection between the two network nodes.

6. Discover, via inquiry or advertisement, other authorized network nodes as they become active and available.

One popular protocol for managing networked devices is the Simple Network Management Protocol [SNMP]. The current standard version, SNMPv3, defines the full security framework including User-based Security Model [USM] and View-based Access Control Model [VACM]. SNMP was designed to facilitate the exchange of management information between networked devices. Even though it was originally intended to configure network equipment, SNMP is mainly being used for network monitoring due to several reasons. Firstly, network operators prefer the text-based Command Line Interfaces (CLI) to configure their boxes, instead of the BER-encoded SNMP (see [BER]). Secondly, many equipment vendors did not provide the option to completely configure their devices via SNMP (see [RFC3535].)

The Network Configuration Protocol [NETCONF] uses an Extensible Markup Language (XML) based data encoding for the configuration data and the protocol messages to provide mechanisms to install, manipulate, and delete the configuration of network devices. The Secure Shell [SSH] protocol is mandatory to support for confidentiality and authentication. NETCONF uses a simple RPC-based mechanism to facilitate communication between a client and a server. A client is typically a network administrator, while a server is typically a network device. Accordingly, a device may optionally support multiple NETCONF sessions but is only required to support one session. After all, "the NETCONF protocol is focused on the information required to get the device into its desired running state" by the network administrator.

Due to the dynamic nature of the virtual network, existing protocols that are geared towards static or manual configuration or monitoring purposes would be difficult, if not impossible, to allow a user to discover important information about the authorized network nodes available. Furthermore, as the number of network nodes increases, the amount of effort required becomes prohibitive for manual configuration.

A protocol to facilitate the automated discovery, management, and configuration of network nodes will be useful in establishing a dynamic virtual network. This protocol does not directly setup a secure connection between the two network nodes. It only conveys the information needed by the two network nodes to setup a secure connection. This enables all existing methods of secure connection

setup, such as VPN, to be supported without any changes. Furthermore, with the desirability of having a central repository for scalability reasons to satisfy the connection and security requirements, the management protocol should support the following interactions between a network node and the central repository:

1. Mutual authentication between a network node and the central repository

2. Virtual address assignment for the network node

3. Responding to inquiries from each network node regarding the online status and other pertinent information related to peer discovery for other network nodes that it is authorized to access

4. Providing all necessary parameters for setting up a secure connection between the two network nodes

5. Initiating State Change Notifications from the network nodes

Multiple central repositories are desirable for redundancy. If the [LDAP] information base is used to support the central repository, then the information can be transferred using the [LDAP] protocol. Otherwise a protocol is needed for distributing the information between central repositories.

## 3 Conclusions

This Problem Statement concludes that to handle the connectivity and security problems related to the task of establishing a virtual network in a dynamic environment between two authorized network nodes, it would be desirable to have a central repository to coordinate the connection process for scalability reasons. Having a central repository facilitates the task of the network administrator by allowing him/her to go beyond a simple node-by-node management model, where each network node is manually and individually configured. Instead, each network node subordinates its discovery and management responsibilities to the central repository. Each network node, having retrieved the information from the central repository regarding the other network nodes that it is authorized to access, can proceed with the connection process using supported standards.

With the central repository being the consolidated configuration point for all the network nodes in the virtual network, a protocol is needed for the interaction between a central repository and a

network node. Where redundancy is required, the protocol also needs to handle the interaction among central repositories.

## 4 Security Considerations

If a new protocol is deployed, the interaction between a central repository and a network node and the interaction between two central repositories is subject to various security threats. As a result, the protocol messages may need to be authenticated. In addition, to protect against snooping of the protocol messages, confidentiality support is desirable and is required when certain functions of the central repository are utilized.

## 5 IANA Considerations

This document has no actions for IANA.

## 6 Informative References

[BER] "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T X.690, July 2002

[DHCP] R. Droms, "Dynamic Host Configuration Protocol", RFC 2131, March 1997

[DNS] P. Mockapetris, "Domain Names - Implementation and Specification", RFC 1035, November 1987

[RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006.

[IATF] Technical Directors, National Security Agency Information Assurance Solutions, "Information Assurance Technical Framework", Release 3.1, September 2002

[IPSEC] S. Kent et al., "Security Architecture for the Internet Protocol", RFC 4301, December 2005

[ISCSI] J. Satran et al., "Internet Small Computer Systems Interface (iSCSI)", RFC 3720, April 2004

[ISNS] J. Tseng et al., "Internet Storage Name Service (iSNS)", RFC 4171, September 2005

[LDAP] K. Zeilenga, "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map", RFC 4510, June 2006

[NAT] P. Srisuresh et al., "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001

[NETCONF] R. Enns, "NETCONF Configuration Protocol", RFC4741, December 2006

[PKCS] J. Jonsson et al., "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003

[RFC3535] J. Schoenwaelder, "Overview of the 2002 IAB Network Management Workshop", RFC 3535, May 2003

[RFC4572] J. Lennox, "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)", RFC 4572, July 2006

[RFC5128] P. Srisuresh et al., "State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs)", RFC 5128, March 2008

[SLP] E. Guttman et al., "Service Location Protocol, Version 2", RFC 2608, June 1999

[SNMP] R. Presuhn et al., "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3416, December 2002

[SSH] T. Ylonen et al., "The Secure Shell (SSH) Protocol Architecture", RFC 4251, January 2006

[TLS] T. Dierks et al., "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008

[TURN] R. Mahy et al., "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", RFC 5766, April 2010

[UDP] J. Postel, "User Datagram Protocol", STD 6, RFC 768, August 1980

[USM] U. Blumenthal et al., "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, December 2002

[VACM] B. Wijnen et al., "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3415, December 2002

[VPN] A. Nagarajan, "Generic Requirements for Provider Provisioned Virtual Private Networks (PPVPN)", RFC 3809, June 2004

## 7 Acknowledgments

The authors would like to thank David Harrington and Linda Dunbar for their valuable advice and suggestion. The authors would also like to thank Margaret Wasserman and Padmanabha Nallur for laying out the groundwork in the earlier submitted IETF drafts related to the subject.

## Author's Address

Michael Ko
Huawei Symantec Technologies Co., Ltd.
20245 Stevens Creek Blvd.
Cupertino, CA 95014, USA
Phone: +1-408-510-7465
Email: michael@huaweisymantec.com

Edward Wang
Huawei Symantec Technologies Co., Ltd.
3rd Floor, Section D, Keshi Building
No. 28A, Xinxi Rd., Shangdi, Haidian Dist.
Beijing 100085 P.R. China
Phone: +86-10-6272-1288
Email: wangyc@huaweisymantec.com

## Copyright Notice

## Intellectual Property Statement



## Disclaimer of Validity