IANS

Service Provider MPLS VPN Security Considerations

IANS CUSTOM REPORT

SEPTEMBER 2011

COMMISSIONED BY:

CERTES NETWORKS

Contents

Executive Summary

Multi-Protocol Labeled Switching (MPLS) has become a foundational protocol component of many service provider networks; MPLS enables enhanced quality of service, flexible redundancy, and provides traffic isolation within IP routing domains. That isolation capability has become an increasingly popular service offering to customers looking to interconnect their private networks with a provider managed MPLS VPN (Virtual Private Network) in which traffic is tunneled across the provider backbone between two MPLS enabled endpoints. Although these types of tunnels often are considered “private” connectivity, these circuits offer customers no degree of confidentiality if the transmission path of the circuit, physical links in intermediate facilities, or administrative domain of the service provider can be compromised.

It has been the tendency of MPLS customers to underrate the likelihood that an attacker can obtain such administrative access. These conceptions are routinely being shattered every day by media coverage of major breaches, breaches which were previously considered by many security professionals to be unlikely. Furthermore it is clear that even detecting a compromise from a sophisticated attacker can be extremely difficult. Breaches often go undetected for months, or even years in many cases. The recent compromises of certificate authorities DigiNotar, GlobalSign, and Comodo are of particular relevance. Not only do they represent “trusted” components of critical infrastructure, but they also increase the value of the targets we are discussing to would be attackers. An ISP backbone router would be an ideal target for an attacker to leverage a compromised SSL CA root certificate to man-in-the-middle a large population of victim sessions. These same routers facilitate MPLS VPN switching for customer traffic.

Many penetration testers and attackers alike are also increasing their focus on physical attacks in which datacenters, intermediate distribution facilities, and customer premises are vulnerable. In customer premise locations, access to the building cabling plants and data closets is often recklessly given to other tenants, third party vendors, and almost anyone claiming to need admittance into these facilities. Other times this infrastructure may be simply unprotected altogether. In this situation an attacker may find it trivial to obtain access to the physical links in either the provider network or the customer uplink, both of which can be exploited with readily available commodity hardware such as copper and fiber optic taps to eaves drop, or even attack these customer networks.

To articulate these threats, this document describes two threat scenarios against a real MPLS VPN environment that was constructed to demonstrate the typical attack surface of an MPLS Layer 3 VPN provider network.

Although MPLS networks offer several advantages over traditional private circuits with regard to cost, scalability, and flexibility of traditional circuits, customers often believe these service offerings fall into a security-equivalency with traditional leased line or dedicated transport options and underestimate the risk of an attack on the service provider network that is outside of their administrative domain. They rely strictly on their trust in the provider to keep attackers out rather than instituting appropriate controls to ensure the confidentiality and integrity of the transmission paths in question.

Fortunately a hybrid approach exists where MPLS VPN links can leverage cryptographically secure tunneling to mitigate these threats with great effectiveness without compromising the other advantages inherent to MPLS service offerings. For most use cases, encryption offers an exceptional level of protection against the types of attacks discussed in this report, with no notable impact on service quality or performance.

Service Provider MPLS VPN Security Considerations

This report examines the security of an externally managed MPLS L3 VPN circuit typical of service provider offerings from the customer perspective.

Both threat scenarios discussed assume that an attacker has gained administrative access to the service provider network and can control provider routers (known as P routers) and/or provider edge routers (known as PE routers), or that an attacker has obtained some type of physical access to the physical links interconnecting any of the customer or provider routers.

Attack Surface of MPLS Provider Networks

Although this document will not demonstrate how an attacker might obtain administrative access to the provider administrative domain, it is important to consider, at a high level, how this might happen.

The attack surface of provider networks typically includes:

- Threats from insiders that have been granted access to the P and PE routers or can somehow obtain access to those routers through physical or logical methods. In many large provider networks, this could be hundreds or perhaps even thousands of users.

- Attackers who have gained access through direct attacks compromising infrastructure services or the routers themselves. These traditional attacks may be the most difficult vector, but have proven historically to be some of the most successful methods of compromising access.

- Attackers who have successfully targeted users with administrative access through client-side attacks such as targeted malware campaigns, spear-phishing attempts, or social engineering. From what has been disclosed to date, this growing threat vector is responsible for some of the most elaborate compromises against hard targets. Within service providers, operations personnel who are managing the critical infrastructure find this to be one of the most likely threat scenarios.

- Physical attacks on provider equipment and physical links in datacenter, colocation facilities, third party facilities, and on customer premises.

Given the very real threats that these networks face, we will explore the potential security impacts of this type of access against a customer network. To do so, we have prepared three threat scenarios that demonstrate the vulnerability of MPLS L3 VPN networks. These attacks were demonstrated using a test environment that was a fully functional model of an MPLS L3 VPN network.

MPLS Background

MPLS (Multi-Protocol Label Switching) is an encapsulation technology used to carry arbitrary data (usually IP packets) across a network. Provider networks typically leverage MPLS to establish independent IP routing domains on their backbone network, and can leverage other associated protocols to enhance switching of MPLS packets, including LDP (Label Distribution Protocol) or RSVP-TE (Resource Reservation Protocol – Traffic Engineering).

For the purposes of this document, it is enough to understand that packets entering the MPLS network are first encapsulated at the MPLS edge (sometimes called the provider edge or PE router) and a label is inserted on these packets, which is then used as an alternative to the IP destination of the packet to deliver the packet, independent of the IP payload, to the destination network.

Upon reaching the destination network, the MPLS label is removed and the packet is routed by the egress MPLS router (the destination PE router) and forwarded on.

This allows a single provider network to carry many independent IP routing domains. As such, customers can maintain overlapping IP address space in their own administrative routing domains without any negative interactions.

Threat Scenarios

The following scenarios will be described through the use of a model MPLS VPN network and from conducting the proposed attacks. Both scenarios we will explore will presume that an attacker has obtained access to the provider administrative domain or obtained access to the link through physical tapping or compromising of a P-PE or PE-CE link. That is, it can control Provider (P) and Provider Edge (PE) routers or traffic.

1. An attacker intercepts a confidential communication transmitted across an MPLS L3 VPN circuit.
2. An attacker leverages access to a provider router to tunnel traffic into a customer MPLS network.

The following diagram depicts the model network constructed:

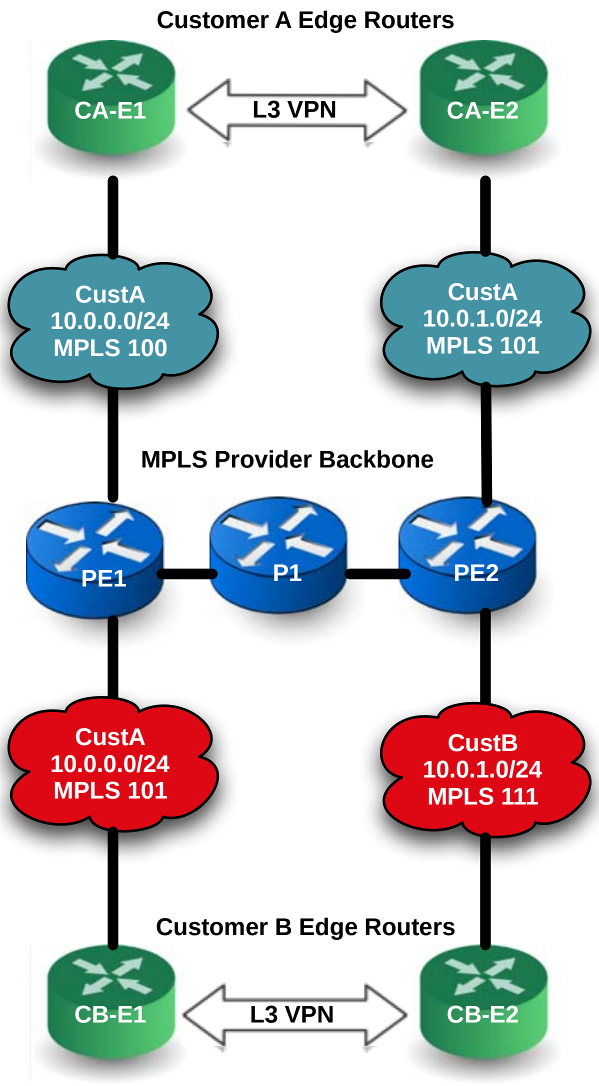


Figure 1 - MPLS L3 VPN Model Network

The PE1, PE2, and P1 routers represented in the diagram were constructed using OpenBSD 4.9. At a high level, the network was constructed in the following way:

1. Three PC systems were installed using OpenBSD 4.9.
2. Ethernet links between P1 and PE1, and P1 and PE2, were established.
3. Loopback interfaces were assigned to each system.
4. The OpenOSPFd was used to establish an OSPF backbone Area 0 across the provider routers.
5. The OpenBSD "ldpd" (label distribution protocol daemon) was used to enable MPLS label switching across the "provider network."
6. MPE (MPLS Provider Edge) interfaces were established for two customers, A & B, using overlapping IP address space:
    a. 10.0.0.0/24 for both customers attached to PE1.
    b. 10.0.1.0/24 for both customers attached to PE2.
7. OpenBGPd was configured to provide MPLS label assignments and exchange label information for each customer routing domain.
8. Four PCs running Ubuntu Linux were installed at each Customer Edge network to represent the "Customer Edge" routers.
9. Connectivity and routing isolation were verified.

Threat Scenario 1: An attacker intercepts a confidential communication transmitted across an MPLS L3 VPN circuit.

Scenario Description of Events:

An email is sent from a user "test" on CA-E1 (The Customer Edge Router attached to PE1) containing the message "Super Secret Test" to test@CA-E2, a mailbox on the remote customer edge router.

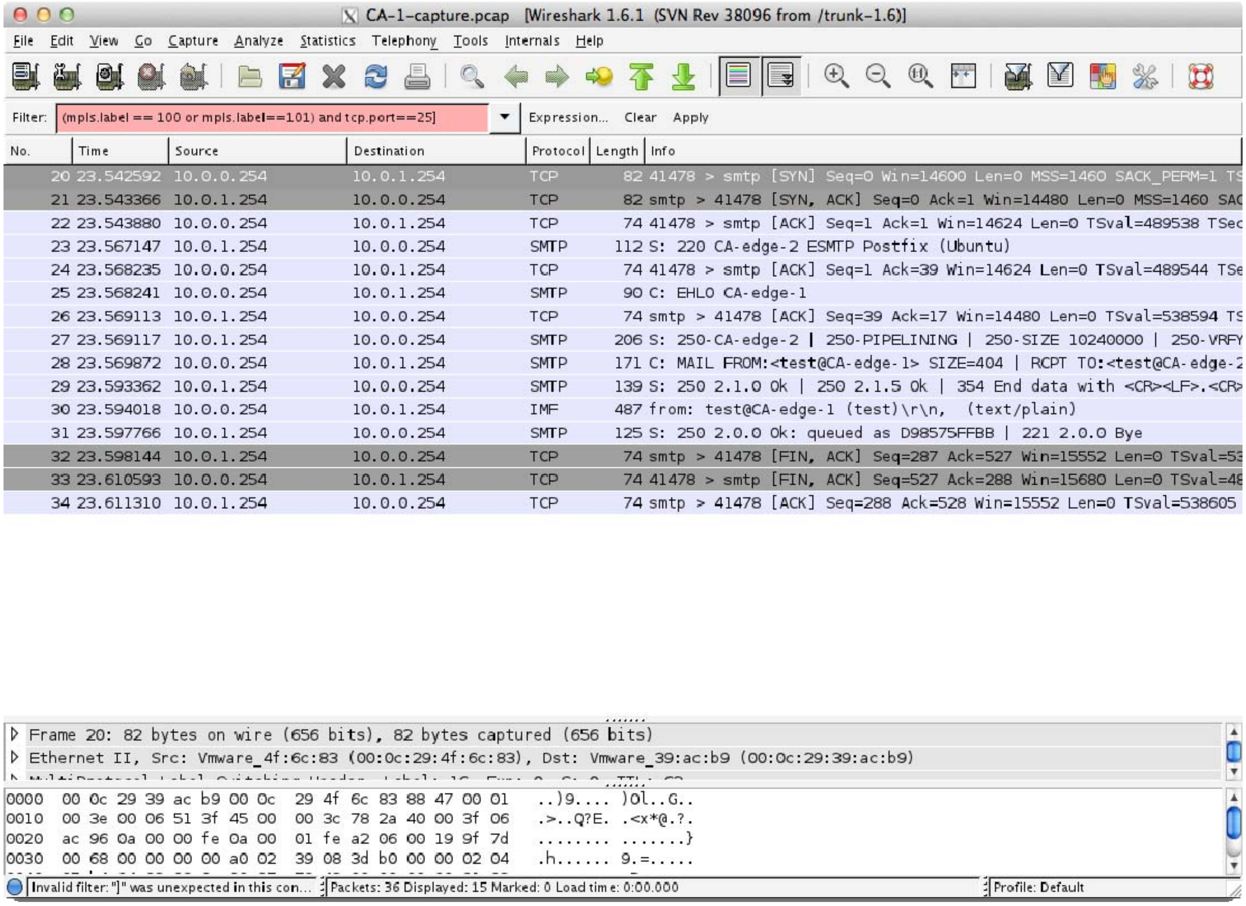
An attacker with administrative privilege on the P1 router captures the traffic on the PE-1 or PE-2 uplink interfaces:

```
p-core-1# tcpdump –s 1524 –n –i vlan10 –w file.pcap
```

It is important to note that this type of threat to confidentiality link is not limited to those with administrative access to the configuration of the device. Provider routers (P and PE), customer equipment (CE), and the physical links interconnecting those devices are also at risk. The physical vulnerability of critical infrastructure emerges as one of the most systemic issues in information security field, and is often not assessed or included in the threat model of information systems. The scenario provided could very easily be adapted to physical attacks where an attacker is able to tap the physical circuits using readily available commodity hardware such as copper and fiber optic taps, or boot attacks against the infrastructure to gain access. In large quantities, evaluating these risks may not be even possible since the service provider or customer may have unfettered access to physical links and data distribution areas within their facility.

Later, an attacker analyzes the resulting capture using the Wireshark protocol analysis tool (http://www.wireshark.org).

He can select the specific SMTP traffic for Customer A using the MPLS destination labels as a search filter in combination with a search filter for TCP port 25:


CA-1-capture.pcap [Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply

Filter: (mpls.label == 100 or mpls.label==101) and tcp.port==25]

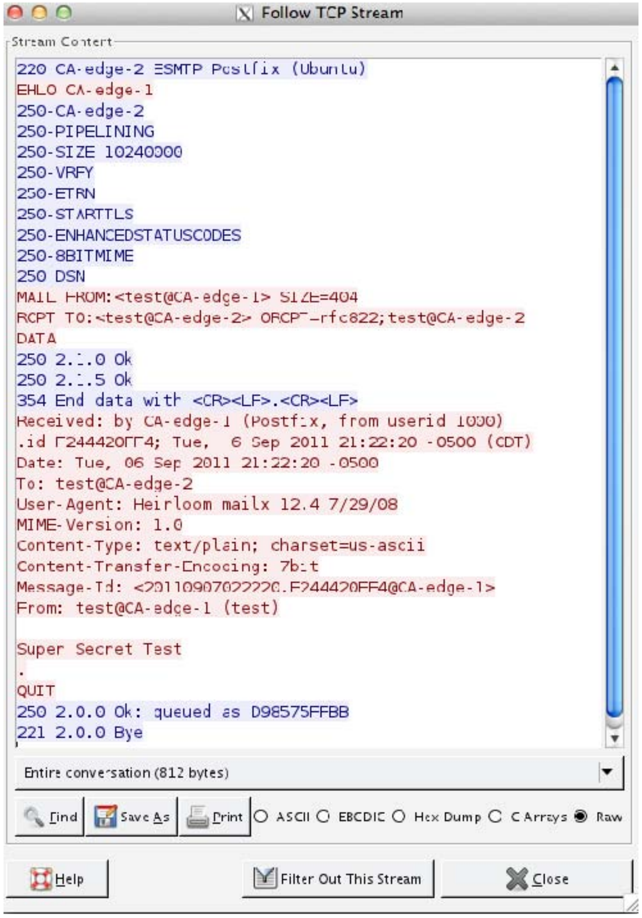
```
No.  Time      Source      Destination  Protocol Length Info
  20 23.542592 10.0.0.254  10.0.1.254   TCP       82 41478 > smtp [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TS
  21 23.543366 10.0.1.254  10.0.0.254   TCP       82 smtp > 41478 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SAC
  22 23.543880 10.0.0.254  10.0.1.254   TCP       74 41478 > smtp [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=489538 TSec
  23 23.567147 10.0.1.254  10.0.0.254   SMTP     112 S: 220 CA-edge-2 ESMTP Postfix (Ubuntu)
  24 23.568235 10.0.0.254  10.0.1.254   TCP       74 41478 > smtp [ACK] Seq=1 Ack=39 Win=14624 Len=0 TSval=489544 TSe
  25 23.568241 10.0.0.254  10.0.1.254   SMTP      90 C: EHLO CA-edge-1
  26 23.569113 10.0.1.254  10.0.0.254   TCP       74 smtp > 41478 [ACK] Seq=39 Ack=17 Win=14480 Len=0 TSval=538594 TS
  27 23.569117 10.0.1.254  10.0.0.254   SMTP     206 S: 250-CA-edge-2 | 250-PIPELINING | 250-SIZE 10240000 | 250-VRFY
  28 23.569872 10.0.0.254  10.0.1.254   SMTP     171 C: MAIL FROM:<test@CA-edge-1> SIZE=404 | RCPT TO:<test@CA-edge-2
  29 23.593362 10.0.1.254  10.0.0.254   SMTP     139 S: 250 2.1.0 Ok | 250 2.1.5 Ok | 354 End data with <CR><LF>.<CR>
  30 23.594018 10.0.0.254  10.0.1.254   IMF      487 from: test@CA-edge-1 (test)\r\n,  (text/plain)
  31 23.597766 10.0.1.254  10.0.0.254   SMTP     125 S: 250 2.0.0 Ok: queued as D98575FFBB | 221 2.0.0 Bye
  32 23.598144 10.0.1.254  10.0.0.254   TCP       74 smtp > 41478 [FIN, ACK] Seq=287 Ack=527 Win=15552 Len=0 TSval=53
  33 23.610593 10.0.0.254  10.0.1.254   TCP       74 41478 > smtp [FIN, ACK] Seq=527 Ack=288 Win=15680 Len=0 TSval=48
  34 23.611310 10.0.1.254  10.0.0.254   TCP       74 smtp > 41478 [ACK] Seq=288 Ack=528 Win=15552 Len=0 TSval=538605
```

```
▷ Frame 20: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
▷ Ethernet II, Src: Vmware_4f:6c:83 (00:0c:29:4f:6c:83), Dst: Vmware_39:ac:b9 (00:0c:29:39:ac:b9)
```

```
0000  00 0c 29 39 ac b9 00 0c  29 4f 6c 83 88 47 00 01   ..)9.... )Ol..G..
0010  00 3e 00 06 51 3f 45 00  00 3c 78 2a 40 00 3f 06   .>..Q?E. .<x*@.?.
0020  ac 96 0a 00 00 fe 0a 00  01 fe a2 06 00 19 9f 7d   ........ .......}
0030  00 68 00 00 00 00 a0 02  39 08 3d b0 00 00 02 04   .h...... 9.=.....
```

Invalid filter: "]" was unexpected in this con... | Packets: 36 Displayed: 15 Marked: 0 Load time: 0:00.000 | Profile: Default

Using the “Wireshark Follow TCP Stream” feature on any packet, he can reassemble the original message:



```
220 CA-edge-2 ESMTP Postfix (Ubuntu)
EHLO CA-edge-1
250-CA-edge-2
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM:<test@CA-edge-1> SIZE=404
RCPT TO:<test@CA-edge-2> ORCPT=rfc822;test@CA-edge-2
DATA
250 2.1.0 Ok
250 2.1.5 Ok
354 End data with <CR><LF>.<CR><LF>
Received: by CA-edge-1 (Postfix, from userid 1000)
.id F244420FF4; Tue,  6 Sep 2011 21:22:20 -0500 (CDT)
Date: Tue, 06 Sep 2011 21:22:20 -0500
To: test@CA-edge-2
User-Agent: Heirloom mailx 12.4 7/29/08
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20110907022220.F244420FF4@CA-edge-1>
From: test@CA-edge-1 (test)

Super Secret Test
.
QUIT
250 2.0.0 Ok: queued as D98575FFBB
221 2.0.0 Bye
```

Here the attacker sees the resulting message: “Super Secret Test”

Scenario 1 Conclusion:

For an attacker with administrative access to the provider edge network, it is a simple matter to reconstruct unencrypted protocols such as e-mail, web, and even voice traffic in IP telephony networks.

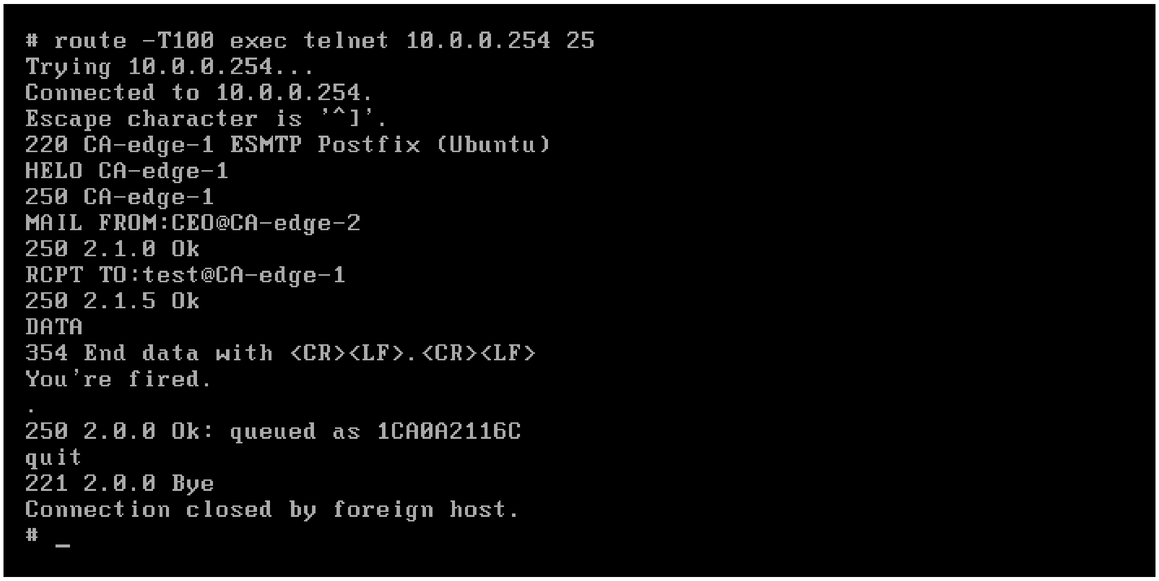
Threat Scenario 2: An attacker leverages access to a provider router to tunnel traffic into a customer MPLS network.

In scenario 1 we explored a passive interception of traffic using common open source packet capture and traffic analysis tools. The objective of this threat scenario is to demonstrate how it is also simple for an attacker who has administrative access to the provider edge (PE) routers to establish connectivity to the customer network.

Scenario Description of Events

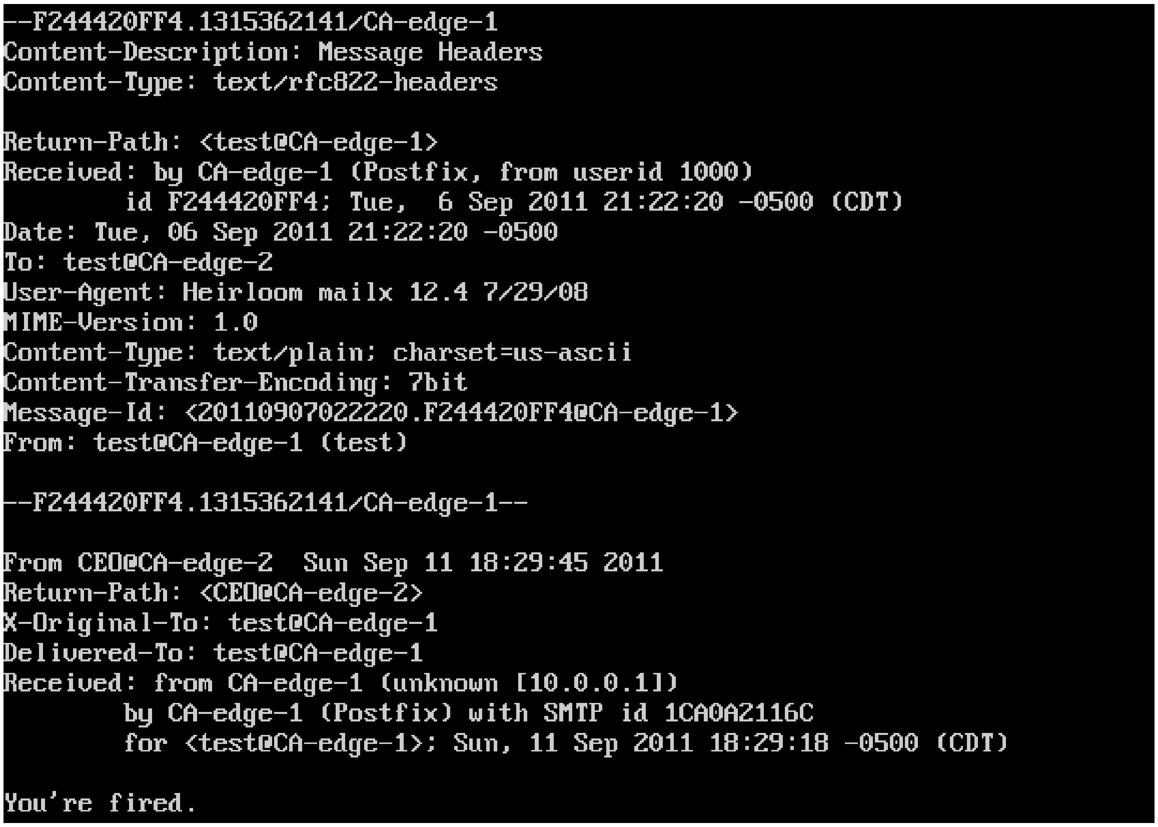
In this scenario we explore the threat of an attacker not only intercepting data in flight, but actually leveraging their physical or administrative access to attack a customer’s network. In this scenario the attacker has the benefit of a PE router running OpenBSD, which is capable of running the nmap port scanning tool. However, similar attacks against Cisco, Juniper, or any more commercially popular provider edge platform would also be trivial. For instance, an attacker with remote access could simply establish a GRE tunnel from their attacking host into the customer routing domain.

The procedure here is simple: the attacker only has to execute the network client he wishes to run in the appropriate routing domain. For example, here we execute a default nmap (a common and powerful open source network port scanner, available at http://nmap.org) against the customer A edge router 1 (CA-E1,10.0.0.254):



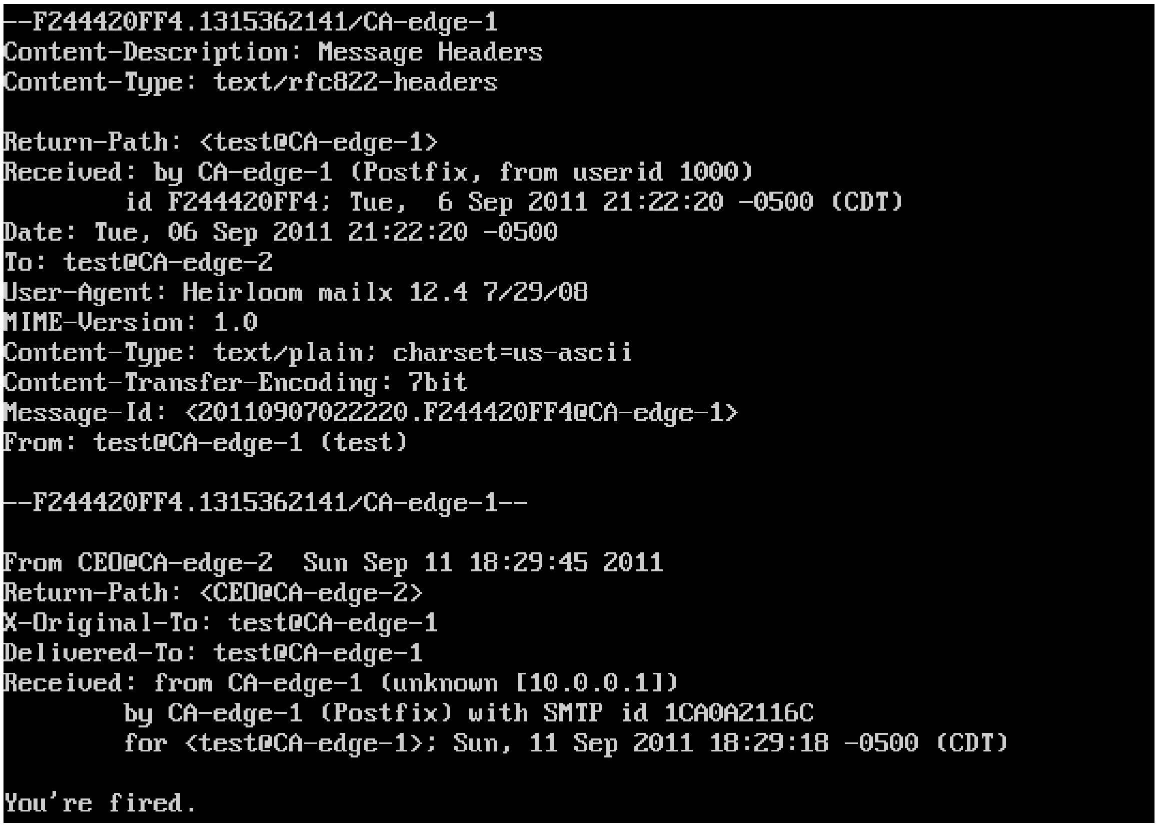
```
# route -T100 exec telnet 10.0.0.254 25
Trying 10.0.0.254...
Connected to 10.0.0.254.
Escape character is '^]'.
220 CA-edge-1 ESMTP Postfix (Ubuntu)
HELO CA-edge-1
250 CA-edge-1
MAIL FROM:CEO@CA-edge-2
250 2.1.0 Ok
RCPT TO:test@CA-edge-1
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
You're fired.
.
250 2.0.0 Ok: queued as 1CA0A2116C
quit
221 2.0.0 Bye
Connection closed by foreign host.
# _
```

Here the attacker discovers two ports that he may use to attack the gateway router or potentially forge mail into the private link, as in the following example:



```
--F244420FF4.1315362141/CA-edge-1
Content-Description: Message Headers
Content-Type: text/rfc822-headers

Return-Path: <test@CA-edge-1>
Received: by CA-edge-1 (Postfix, from userid 1000)
        id F244420FF4; Tue,  6 Sep 2011 21:22:20 -0500 (CDT)
Date: Tue, 06 Sep 2011 21:22:20 -0500
To: test@CA-edge-2
User-Agent: Heirloom mailx 12.4 7/29/08
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20110907022220.F244420FF4@CA-edge-1>
From: test@CA-edge-1 (test)

--F244420FF4.1315362141/CA-edge-1--

From CEO@CA-edge-2  Sun Sep 11 18:29:45 2011
Return-Path: <CEO@CA-edge-2>
X-Original-To: test@CA-edge-1
Delivered-To: test@CA-edge-1
Received: from CA-edge-1 (unknown [10.0.0.1])
        by CA-edge-1 (Postfix) with SMTP id 1CA0A2116C
        for <test@CA-edge-1>; Sun, 11 Sep 2011 18:29:18 -0500 (CDT)

You're fired.
```

The resulting mail message in the spool file for test@CA-E1:



```
--F244420FF4.1315362141/CA-edge-1
Content-Description: Message Headers
Content-Type: text/rfc822-headers

Return-Path: <test@CA-edge-1>
Received: by CA-edge-1 (Postfix, from userid 1000)
        id F244420FF4; Tue,  6 Sep 2011 21:22:20 -0500 (CDT)
Date: Tue, 06 Sep 2011 21:22:20 -0500
To: test@CA-edge-2
User-Agent: Heirloom mailx 12.4 7/29/08
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20110907022220.F244420FF4@CA-edge-1>
From: test@CA-edge-1 (test)

--F244420FF4.1315362141/CA-edge-1--

From CEO@CA-edge-2  Sun Sep 11 18:29:45 2011
Return-Path: <CEO@CA-edge-2>
X-Original-To: test@CA-edge-1
Delivered-To: test@CA-edge-1
Received: from CA-edge-1 (unknown [10.0.0.1])
        by CA-edge-1 (Postfix) with SMTP id 1CA0A2116C
        for <test@CA-edge-1>; Sun, 11 Sep 2011 18:29:18 -0500 (CDT)

You're fired.
```

Scenario 2 Conclusion:

This scenario demonstrated that compromising the integrity of the network was just as simple as compromising the confidentiality of the data in-flight over the network. An attacker was able to launch nmap scans as well as forge e-mail within the customer network from the PE router.

Conclusion

Managed MPLS VPN networks provide a cost effective and flexible alternative to dedicated high-speed fiber optics networks, however many customers underestimate the threats to provider networks and physical infrastructure that these circuits rely on. In assessing the threats against these circuits, it is usually difficult or impossible to obtain enough information to determine whether the circuit can be treated with a level of trust beyond that of a traditional public IP path. Those considering leveraging these circuits for any type of sensitive transit should seek out additional controls.

Fortunately a variety of solutions exist that can provide line-rate end-to-end cryptographic protection of these links without compromising the performance characteristics of the circuit. These solutions operate transparently at the endpoints, maintaining the simplicity offered by service provider managed MPLS VPN solutions. It is highly recommended that these products be considered for hybrid deployment of any existing or future MPLS VPN channel that is not used exclusively for public IP transport.

Analyst Reactions

“After realizing the attacks described against the model network, it is clear that for links requiring any level of confidentiality and integrity beyond that of your typical public IP transit network, customers should seek out a strong encryption solution to protect the MPLS tunnel path between their customer edge routers. Relying on the ISP to protect the attack surface of these links at the same level for which physical security can be maintained for traditional leased lines is simply not acceptable for most applications leveraging MPLS VPN networks.”

- Kevin A. Nassery, U.S. Bank, Manager of Attack & Penetration Testing

"It's definitive; the Emperor's clothes were never present to begin with. As someone who's had numerous discussions over the years about the theoretical security of WAN links, this paper shows the practical reality: without encryption, there are a substantial set of threat scenarios and vectors that could lead to trivial compromise of sensitive communications. Don't rely on the assumption of unlikelihood - take control of your risk by deploying encryption across untrusted networks."

- Joel Scambray, Cigital Inc., Managing Principal and Co-Author of “Hacking Exposed”.

"When looking to move to an MPLS VPN solution, many customers downplay the threats to the security of the transmission path and instead put their full trust in the security of the service provider. The attacks shown in this report make it clear that MPLS VPN customers who need confidentiality and integrity beyond what a public network provides must look to implement some form of encryption at the endpoints to provide complete protection."

- Brandon Knight, Amazon, Senior Security Engineer

About Certes Networks

Certes Networks is the leader in scalable security solutions for high performance networks. Our encryption solutions secure data over any wide area network, data center, or public/private cloud without compromising network availability, application performance, or operational visibility. We help our customers to reduce the risk of data theft or loss without forcing infrastructure changes or performance downgrades.

About IANS

IANS is the leading provider of in-depth security insights delivered through its research, community, and consulting offerings. Fueled by interactions among IANS Faculty and end users, IANS provides actionable advice to information security, risk management, and compliance executives. IANS powers better and faster technical and managerial decisions through experience-driven advice.

IANS was founded in June 2001 as the Institute for Applied Network Security. Inspired by the Harvard Business School experience of interactive discussions driving collective insights, IANS adapted that format to fit the needs of information security professionals.