

ネットワークのおべんきよしませんか？
ネットワークスペシャリスト[旧テクニカルエンジニア(ネットワーク)]
午後完全解説 Sample

午後Ⅱ問 1 分散オフィスの構築 設問 2

解答

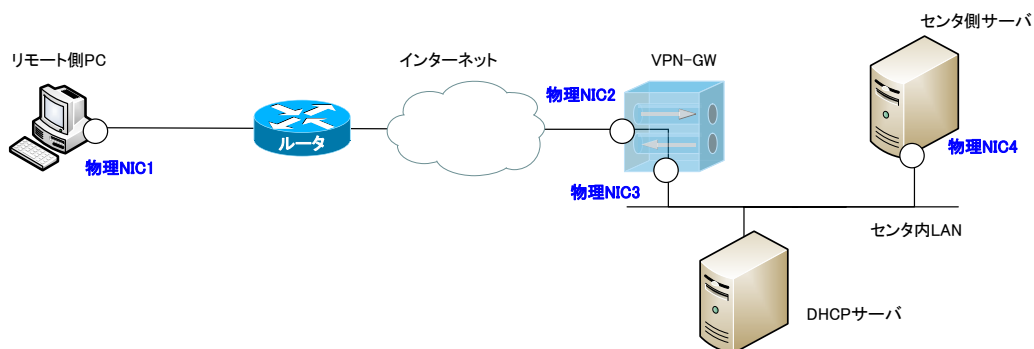
- (1) ソフト NIC と物理 NIC4
- (2) E1 と DT
- (3) E1 のあて先 MAC アドレス : MAC5
P1 のあて先 IP アドレス : IP3
- (4) ①どこからでもアクセスが可能であるから
②使用するアプリケーションに制限がないから

解説

(1)

問題文 図 2 に SSL-VPN レイヤ 2 フォワード方式による仮想イーサネットのデータ転送の様子が記されています。この図は、ごちゃごちゃしてわかりにくいので分かりやすくしましょう。物理的な構成と仮想イーサネットの構成を分けて考えると次のようになります。

【物理的な構成】



【仮想イーサネット構成】

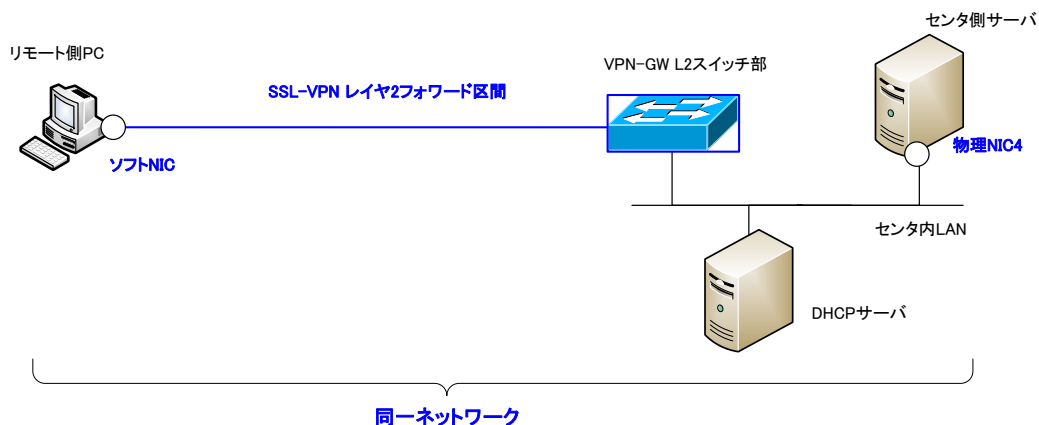


図 1 物理的な構成と仮想イーサネットの構成

VPN や VLAN を利用すると、物理的なネットワーク構成と実質的なネットワーク構成が異なるので、その対応をしっかりと考えることがポイントです。

この図にあるように SSL-VPN レイヤ 2 フォワードの仮想イーサネット構成で、リモート側 PC はソフト NIC で VPN-GW の L2 スイッチ部分に直結されているとみなすことができます。VPN-GW の L2 スイッチ部分は、センタ内 LAN と接続されています。つまり、リモート側 PC、DHCP サーバ、センタ側サーバがすべて同じ L2 スイッチに接続されていることになります。そのため、VPN-GW の L2 スイッチ部分は、リモート側 PC のソフト NIC と DHCP サーバ、センタ側サーバの MAC アドレスを学習して、MAC アドレスベースでイーサネットフレームの転送を行います。

問題文に記されている NIC で、VPN-GW の L2 スイッチ部分が学習する MAC アドレスは「ソフト NIC」と「物理 NIC4」です。

(2)(3)

仮想イーサネット構成のイーサネットフレームがどのようなフォーマットで物理的なネットワーク構成上で転送されるかを考えます。問題文 図 2 は、リモート側 PC からセンタ側サーバへのイーサネットフレームの転送についても記述しています。順を追って、どのようなフォーマットでリモート側 PC のイーサネットフレームがセンタ側サーバへと転送されるかについて解説します。

センタ側サーバと通信するリモート側 PC のアプリケーションのデータは、ソフト NIC から送信されます。レイヤ 3 以上のデータ(DT)にイーサネットヘッダ(E1)を付加して、ソフト NIC から送信します。E1 のヘッダ内のアドレス情報は、次のようになります。

- ・ 送信先 MAC アドレス : MAC5(センタ側サーバ 物理 NIC4)
- ・ 送信元 MAC アドレス : MAC1(リモート側 PC ソフト NIC)

※ 問題文では省略されていますが、送信先 MAC アドレスを解決するために ARP を行っているはずですが。

ソフト NIC から出力されたイーサネットフレーム(E1+DT)を SSL でカプセル化することで、物理的なネットワーク構成上で VPN-GW まで転送できるようにします。

ネットワークのおべんきよしませんか？
ネットワークスペシャリスト[旧テクニカルエンジニア(ネットワーク)]
午後完全解説 Sample

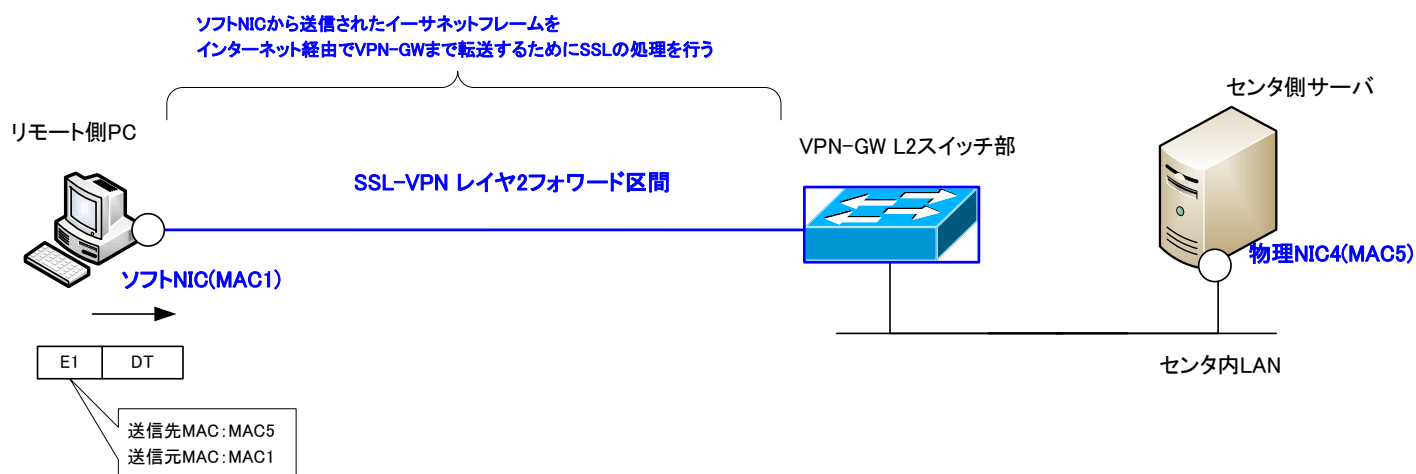


図 2 ソフト NIC からのイーサネットフレームの送信

ソフト NIC から送信されたイーサネットフレームは、まず SSL で暗号化されます。つまり、暗号化されるのは、E1+DT です。そして、SSL/TCP ヘッダ(V1+T1)でカプセル化します。さらに VPN-GW へ IP で転送するための IP ヘッダ(P1)でカプセル化して、物理 NIC1 から送信します。物理 NIC1 から送信する際には、さらにイーサネットヘッダ(E2)をカプセル化します。このときの IP ヘッダ P1 のアドレス情報は、次のようになります。

- ・ 送信先 IP アドレス : IP3(VPN-GW 物理 NIC2)
- ・ 送信元 IP アドレス : IP2(リモート側 PC 物理 NIC1)

また、イーサネットヘッダ E2 のアドレス情報は、次のようになります。

- ・ 送信先 MAC アドレス : ルータ
- ・ 送信元 MAC アドレス : MAC2(リモート側 PC 物理 NIC1)

※ リモート側 PC と VPN-GW は、物理的な構成では別々のネットワークなので、VPN-GW への IP パケットを送信するには、まずデフォルトゲートウェイに送ります。リモート側 PC の物理 NIC1 にはデフォルトゲートウェイとしてルータの IP アドレスが設定されているはずです。

ネットワークのおべんきよしませんか？
 ネットワークスペシャリスト[旧テクニカルエンジニア(ネットワーク)]
 午後完全解説 Sample

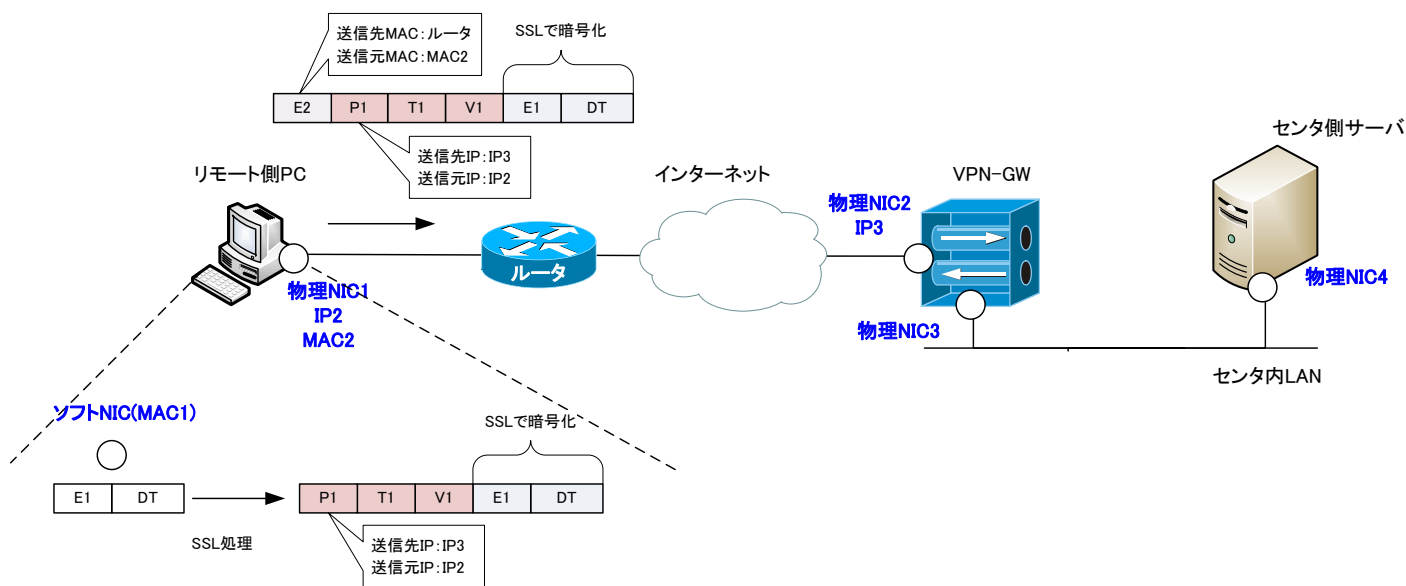


図 3 物理 NIC1 からのイーサネットフレームの送信

このように、ソフト NIC から送信されたイーサネットフレームは SSL で暗号化とカプセル化されて物理 NIC1 から送信されます。物理 NIC1 から送信されたパケットの送信元 IP アドレス IP2 は、プライベートアドレスです。インターネット上を転送するために、ルータで NAT(NAPT)変換を行い IP/TCP ヘッダ(P1+T1)を書き換えて、P2+T2 とします。ルータからインターネットへ送信するためには、何らかのレイヤ 2 ヘッダが付加されます。ただ、このレイヤ 2 ヘッダは問題文からは読み取ることができません。

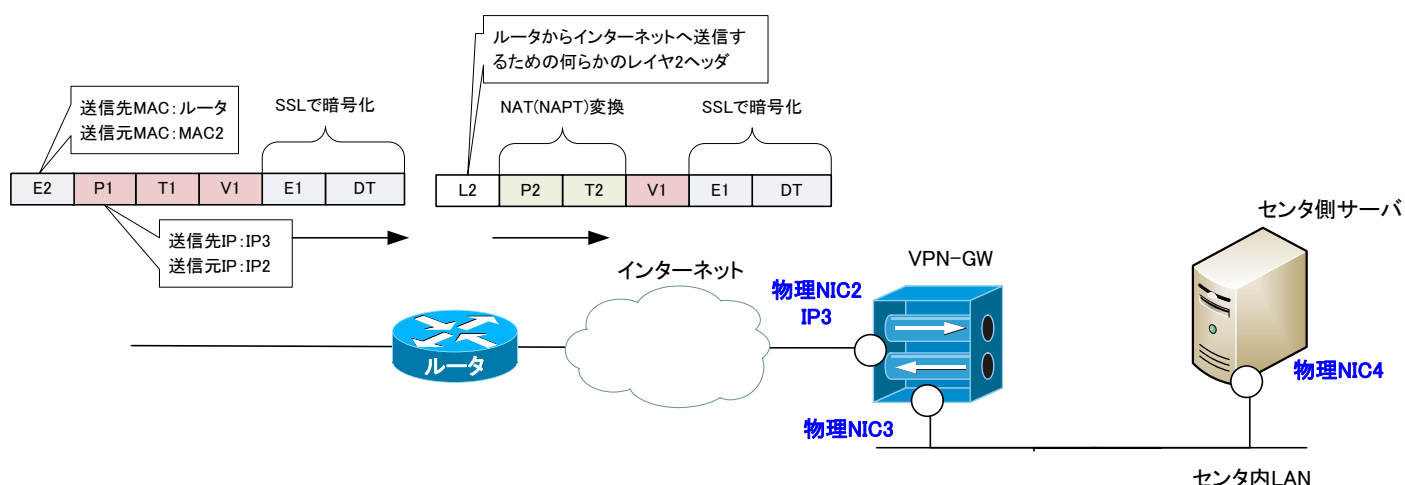


図 4 ルータでの IP/TCP ヘッダの変換

ネットワークのおべんきよしませんか？
ネットワークスペシャリスト[旧テクニカルエンジニア(ネットワーク)]
午後完全解説 Sample

NAPT 変換されたパケットがインターネット上でルーティングされ、VPN-GW まで到達します。VPN-GW で IP/TCP/SSL ヘッダ(P2+T2+V1)のカプセル化を解除し、元のイーサネットフレーム(E1+DT)を復号します。そして、イーサネットフレームをセンタ側サーバへと転送します。この転送は、レイヤ 2 スwitching です。つまり、送信先 MAC アドレス(MAC5)と VPN-GW L2 スwitch 部分の MAC アドレステーブルによって物理 NIC3 へ元のイーサネットフレーム(E1+DT)を転送します。

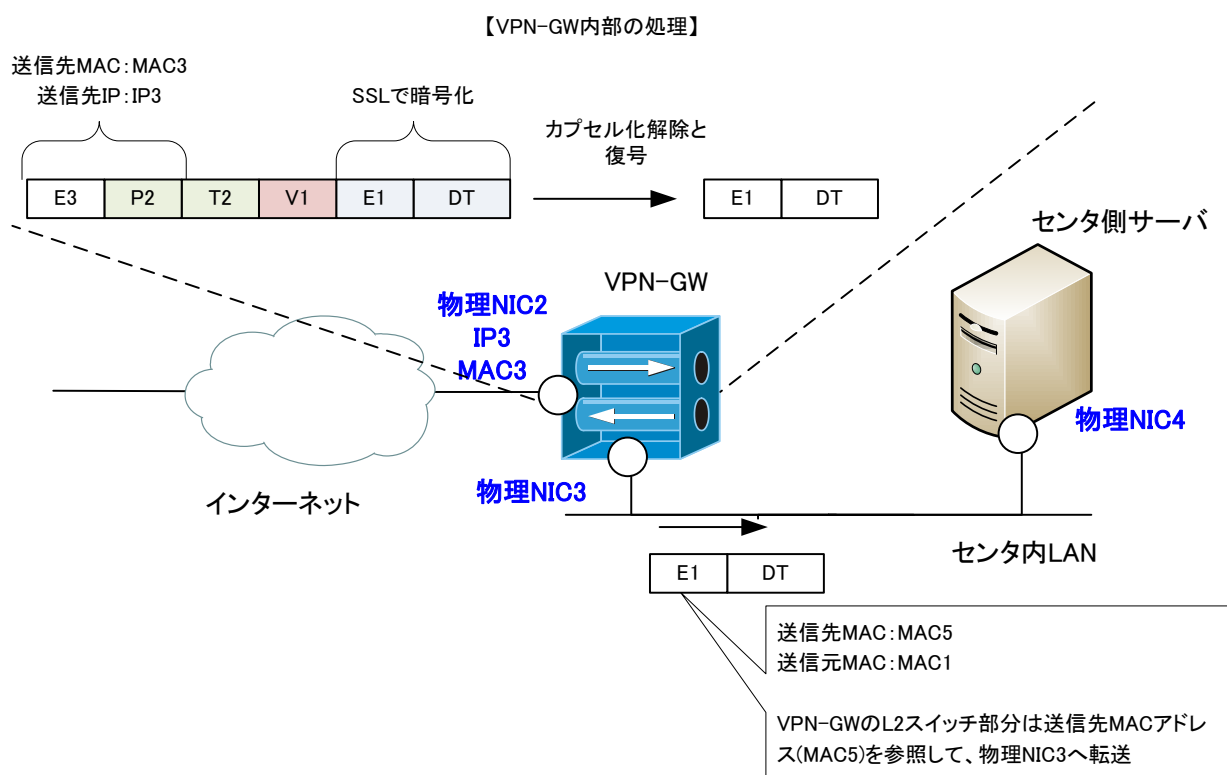


図 5 VPN-GW でのイーサネットフレームの処理

このような仕組みで、リモート側 PC のソフト NIC から送信されたイーサネットフレームをそっくりそのままセンタ側サーバへ転送することができます。

以上を踏まえて解答を考えます。

(2)

SSL で暗号化されるのは、SSL ヘッダの後の部分です。ソフト NIC から送信されるイーサネットフレーム E1+DT が暗号化対象です。

ネットワークのおべんきよしませんか？
ネットワークスペシャリスト[旧テクニカルエンジニア(ネットワーク)]
午後完全解説 Sample

(3)

E1 のあて先 MAC アドレスは、センタ側サーバの物理 NIC4 の MAC アドレス MAC5 です。また、P1 のあて先 IP アドレスは VPN-GW のインターネット側の NIC である物理 NIC2 の IP アドレス IP3 です。

(4)

S 社の要件である出張先などから電子メールや VoIP による内線電話など利用できるようにするために、インターネット VPN の導入を検討しています。設問 1 では、次の 3 つの方式のインターネット VPN を検討しました。

- ・ PPTP
- ・ IPSec-VPN
- ・ 単純な SSL-VPN

これらでは、要件を満たせなかった項目を考えれば解答になります。

PPTP は、PPP フレームでカプセル化した IP パケットをインターネット上で安全に転送できます。そのため、アプリケーションには制限がありません。S 社の要件である電子メールや VoIP などを PPTP 経由で利用することができます。ただし、リモート側がプライベートアドレスである場合、リモート側のルータに PPTP パススルーの機能が必要です。PPTP パススルーの機能がなければ、NAT(NAPT)変換を正常に行うことができず PPTP の通信できません。そのためホテルや喫茶店などからは、社内ネットワークに接続できない可能性があり、どこからでも PPTP でアクセスできるとは限りません。

同じことが IPSec-VPN でも言えます。IPSec は IP パケットを暗号化して安全にインターネット上で転送するので、利用するアプリケーションの制限がありません。ただし、NAT(NAPT)経由で IPSec-VPN の通信を行うには NAT トラバーサル機能が必要です。そのため、この機能がない環境ではどこからでも IPSec-VPN でアクセスできるとは限りません。

一方、SSL-VPN は NAT(NAPT)経由の通信でもルータに特別な機能は必要ありません。SSL-VPN を利用すれば、どこからでも社内のネットワークにアクセスすることができます。ですが、SSL-VPN は UDP を利用するアプリケーションを扱うことができません。VoIP は UDP を利用しているので、SSL-VPN では VoIP による内線電話ができないなどのアプリケーションの制約があります。

設問 2 で検討している SSL-VPN レイヤ 2 フォワードによる仮想イーサネットの構成では、

ネットワークのおべんきよしませんか？
ネットワークスペシャリスト[旧テクニカルエンジニア(ネットワーク)]
午後完全解説 Sample

イーサネットフレームをインターネット上で安全に転送できます。そのため、アプリケーションの制約がありません。電子メールでも VoIP による内線電話でも扱うことができます。また、イーサネットフレームを IP/TCP/SSL でカプセル化するので、通常の NAT(NAPT) 変換を問題なく行うことができます。ルータに特別な機能が必要ないので、どこからでも社内ネットワークへのアクセスが可能であると言えます。

以上の「アプリケーションに制限がない」ということと「どこからでもアクセス可能である」ことの2点が SSL-VPN レイヤ 2 フォワード方式を採用する主な理由です。

参考 URL

- ・ 新機能続々！「SSL-VPN」/キーマンズネット
<http://www.keyman.or.jp/3w/prd/08/30000908/>