PIX/ASA 7.x 및 IOS:VPN 단편화

목차

소개

이 문서에서는 패킷의 단편화로 발생할 수 있는 문제를 완화하는 데 필요한 단계를 안내합니다.프래그먼트화 문제의 한 예는 네트워크로 연결된 자원을 ping하는 기능이지만 E-메일이나 데이터베이스와 같은 특정 애플리케이션을 사용하여 동일한 리소스에 연결할 수 없다는 것입니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

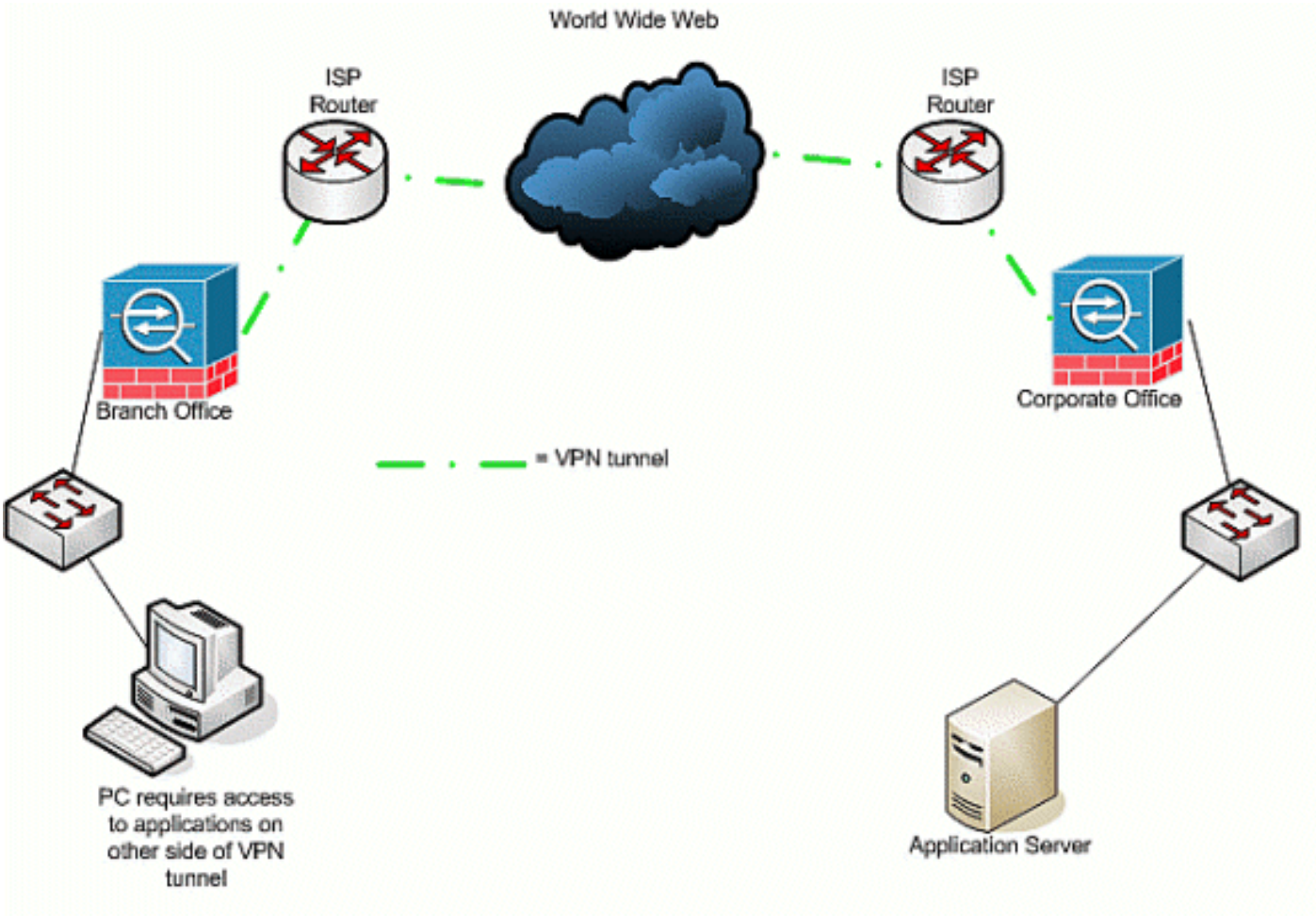
- VPN 피어 간 연결

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



관련 제품

이 컨피그레이션은 다음 하드웨어 및 소프트웨어 버전과 함께 사용할 수도 있습니다.

- IOS 라우터
- PIX/ASA 보안 디바이스

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

IP는 IP 패킷에 대해 최대 길이 65,536바이트를 지원하지만 대부분의 데이터 링크 레이어 프로토콜은 MTU(Maximum Transmission Unit)라고 하는 훨씬 더 작은 길이를 지원합니다. 지원되는 MTU를 기반으로 특정 데이터 링크 레이어 미디어 유형을 통해 전송하려면 IP 패킷을 분리(프래그먼트)해야 합니다.그런 다음 목적지는 프래그먼트를 다시 완전한 원래 IP 패킷으로 재조합해야 합니다.

Protocol	Additional Bytes
ESP (encryption and hash)	56
AH	24+
GRE	24
NAT-T/IPsec over UDP (UDP part)	8
IPsec over TCP (TCP part)	20
L2TP	12
PPTP	48
Outer IP header in IPsec tunnel mode or PPTP/L2TP	20
PPPoE	8

VPN을 사용하여 두 VPN 피어 간의 데이터를 보호할 때 추가 오버헤드가 원래 데이터에 추가되며, 이러한 프래그먼트화가 발생할 수 있습니다.이 표에는 VPN 연결을 지원하기 위해 보호된 데이터에 추가해야 할 수 있는 필드가 나열되어 있습니다.여러 프로토콜이 필요할 수 있으며, 이렇게 하면 원래 패킷의 크기가 커집니다.예를 들어 GRE 터널을 구현한 두 Cisco 라우터 간에 L2L DMVPN IPSEC 연결을 사용하는 경우 다음과 같은 추가 오버헤드가 필요합니다.ESP, GRE 및 외부 IP 헤더 .트래픽이 주소 디바이스를 통과할 때 VPN 게이트웨이에 IPSec 소프트웨어 클라이언트 연결이 있는 경우, 터널 모드 연결을 위한 외부 IP 헤더뿐만 아니라 NAT-T(Network Address Translation-Traversal)에 대한 추가적인 오버헤드가 필요합니다.

단편화 문제

소스가 목적지로 패킷을 전송하면 중간 디바이스에 의한 패킷 조각화에 영향을 주는 IP 헤더의 제어 플래그 필드에 값을 배치합니다.컨트롤 플래그는 길이가 3비트이지만 프래그먼트화에는 처음 2비트만 사용됩니다.두 번째 비트가 0으로 설정된 경우 패킷이 조각화될 수 있습니다.1로 설정된 경우 패킷을 프래그먼트화할 수 없습니다.두 번째 비트는 일반적으로 *DF*(*Don't Fragment*) 비트라고 합니다.세 번째 비트는 프래그먼트화가 발생하는 시기, 조각화된 이 패킷이 마지막 프래그먼트인지(0으로 설정) 또는 패킷을 구성하는 프래그먼트가 더 있는지(1로 설정) 여부를 지정합니다.

프래그먼트화가 필요할 때 문제를 일으킬 수 있는 영역은 4가지입니다.

- 프래그먼트화 및 리어셈블리를 수행하는 두 디바이스에서 CPU 주기 및 메모리의 추가 오버헤드가 필요합니다.
- 목적지로 가는 도중에 하나의 프래그먼트가 삭제되면 패킷을 리어셈블할 수 없으며 전체 패킷을 프래그먼트화하고 다시 전송해야 합니다.이렇게 하면 추가 처리량 문제가 발생합니다. 특히 문제의 트래픽이 속도 제한이 있고, 소스에서 허용 한도를 초과하는 트래픽을 전송하는 경우.
- 패킷 필터링 및 스테이트풀 방화벽은 프래그먼트를 처리하는 데 어려움을 겪을 수 있습니다.프래그먼트화가 발생하면 첫 번째 프래그먼트에는 외부 IP 헤더, 내부 헤더(예: TCP, UDP, ESP 등) 및 페이로드의 일부가 포함됩니다.원래 패킷의 후속 조각은 외부 IP 헤더와 페이로드의 연속.이 프로세스의 문제는 지능적인 필터링 결정을 내리기 위해 특정 방화벽이 모든 패킷의 내부 헤더 정보를 확인해야 한다는 것입니다.해당 정보가 누락되면 첫 번째 프래그먼트를 제외하고 실수로 모든 프래그먼트를 삭제할 수 있습니다.

- 패킷의 IP 헤더에 있는 소스는 세 번째 제어 비트를 *Don't fragment*로 설정할 수 있습니다. 즉, 중간 디바이스가 패킷을 수신하여 프래그먼트화해야 하는 경우 중간 디바이스가 패킷을 프래그먼트화할 수 없습니다.대신 중간 디바이스가 패킷을 삭제합니다.

주 작업

조각화 검색

대부분의 네트워크는 기본 MTU 값이 1,500바이트인 이더넷을 사용하며, 일반적으로 IP 패킷에 사용됩니다.프래그먼트화가 발생하는지 또는 필요하나 수행할 수 없는지(DF 비트가 설정되어 있음) 확인하려면 먼저 VPN 세션을 활성화합니다.그런 다음 이 4가지 절차 중 하나를 사용하여 프래그먼트화를 검색할 수 있습니다.

1. 다른 끝에 있는 디바이스를 ping합니다.이는 터널을 통해 Ping이 허용된다는 가정 하에 있습니다.이 경우 동일한 디바이스에서 애플리케이션에 액세스하십시오.예를 들어 Microsoft 전자 메일 또는 원격 데스크톱 서버가 터널을 통해 있는 경우 Outlook을 열고 전자 메일을 다운로드하거나 원격 데스크톱을 서버에 다운로드해 보십시오.이 방법이 제대로 작동하지 않고 정확한 이름 확인이 있는 경우 프래그먼트화가 문제가 될 가능성이 높습니다.
2. Windows 디바이스에서 다음을 사용합니다.C:\> **ping -f -l packet_size_in_bytes destination_IP_address**.**-f** 옵션은 패킷을 조각화할 수 없도록 지정하는 데 사용됩니다.**-l** 옵션은 패킷의 길이를 지정하는 데 사용됩니다.먼저 패킷 크기가 1,500인 패킷을 사용해 보십시오. 예를 들어 ping**-f -l 1500 192.168.100**입니다. 조각화가 필요하지만 수행할 수 없는 경우 다음과 같은 메시지가 표시됩니다.*패킷은 프래그먼트화되지만 DF가 설정되어 있어야 합니다.*
3. Cisco 라우터에서 debug **ip icmp** 명령을 실행하고 **extended ping** 명령을 사용합니다 .*ICMP:dst(x.x.x.x) 프래그먼트화가 필요한 경우 DF 세트, 연결할 수 없는 경우 y.y.y로 전송됨*, 여기서 x.x.x.x는 대상 디바이스이고 y.y.y.y는 라우터인 경우, 중간 디바이스는 프래그먼트화가 필요하다는 것을 알려주며, 에코 요청에서 DF 비트를 설정했으므로 중간 디바이트가 프래그먼트하여 다음 홉으로 전달할 수 없습니다.이 경우 효과가 있는 ping을 찾을 때까지 ping의 MTU 크기를 점진적으로 줄입니다.
4. Cisco Security Appliances에서 캡처 필터를 사용합니다.ciscoasa (config)#`access-list outside_test permit tcp any host 172.22.1.1 eq 80`**참고:** 소스를 *any*로 남겨 두면 관리자가 NAT(네트워크 주소 변환)를 모니터링할 수 있습니다.ciscoasa (config)#`access-list outside_test permit tcp host 172.22.1.1 eq 80 any`**참고:** 소스 및 목적지 정보를 반대로 하면 반환 트래픽을 캡처할 수 있습니다.`ciscoasa (config)# capture outside_interface access-list outside_test interface outside`사용자는 애플리케이션 X로 새 세션을 시작해야 합니다. 사용자가 새 애플리케이션 X 세션을 시작한 후 ASA 관리자는 **show capture outside_interface** 명령을 실행해야 합니다.

프레임워크 문제에 대한 솔루션

단편화로 문제를 해결할 수 있는 여러 가지 방법이 있습니다.이 섹션에서는 이에 대해 설명합니다.

방법 1:정적 MTU 설정

정적 MTU 설정은 조각화 문제를 해결할 수 있습니다.

1. **라우터의 MTU 변경:**디바이스에서 MTU를 수동으로 설정하면 VPN 게이트웨이 역할을 하는

디바이스에 수신된 패킷이 보호되고 터널을 통해 전송되기 전에 프래그먼트화하도록 지시합니다.라우터가 트래픽을 보호한 다음 프래그먼트화하도록 하는 것이 좋으나, 디바이스가 프래그먼트화합니다.**경고:** 디바이스 인터페이스에서 MTU 크기를 변경하면 해당 인터페이스에서 모든 터널이 종료되고 재구축됩니다.Cisco 라우터에서 **ip** mtucommand를 사용하여 VPN이 종료되는 인터페이스의 MTU 크기를 조정합니다.

```
router (config)# interface type [slot_#/] port_#
router (config-if)# ip mtu MTU_size_in_bytes
```

2. **ASA/PIX의 MTU 변경:**ASA/PIX 디바이스에서 mtucommand를 사용하여 전역 컨피그레이션 모드에서 MTU 크기를 조정합니다.기본적으로 MTU는 1500으로 설정됩니다.예를 들어 보안 어플라이언스에 이름이 *Outside(VPN이 종료됨)인* 인터페이스가 있고, *프래그먼트* 크기로 1380을 사용하려는(Discover Fragmentation 섹션에 나열된 측정을 통해) 다음 명령을 사용합니다.

```
security appliance (config)# mtu Outside 1380
```

방법 2:TCP 최대 세그먼트 크기

TCP 최대 세그먼트 크기는 프래그먼트화 문제를 해결할 수 있습니다.

참고: 이 기능은 TCP에서만 작동합니다.다른 IP 프로토콜은 IP 단편화 문제를 해결하기 위해 다른 솔루션을 사용해야 합니다.라우터에서 ip mtu를 설정하더라도 TCP MSS를 사용하는 TCP 3방향 핸드셰이크 내에서 두 엔드 호스트가 협상하는 것에 영향을 주지 않습니다.

1. **라우터의 MSS 변경:**TCP 트래픽은 일반적으로 대량의 데이터를 전송하는 데 사용되기 때문에 프래그먼트화는 TCP 트래픽에서 발생합니다.TCP는 TCP MSS(Maximum Segment Size)라는 기능을 지원합니다. 이 기능을 통해 두 디바이스에서 TCP 트래픽에 적합한 크기를 협상할 수 있습니다.MSS 값은 각 디바이스에서 정적으로 구성되며 예상 패킷에 사용할 버퍼 크기를 나타냅니다.두 개의 디바이스가 TCP 연결을 설정할 때 3방향 핸드셰이크 내에서 로컬 MSS 값과 로컬 MTU 값을 비교합니다.둘 중 더 낮은 것은 원격 피어로 전송됩니다.그런 다음 두 피어가 교환된 값 중 낮은 값을 사용합니다.이 기능을 구성하려면 다음을 수행합니다.Cisco 라우터에서 VPN이 종료되는 인터페이스에서 **tcp adjust-mss** 명령을 사용합니다.

```
router (config)# interface type [slot_#/] port_#
router (config-if)# ip tcp adjust-mss MSS_Size_in_bytes
```

2. **ASA/PIX에서 MSS 변경:**최대 TCP 세그먼트 크기가 사용자가 설정한 값을 초과하지 않고 최대값이 지정된 크기보다 작지 않은지 확인하려면 글로벌 컨피그레이션 모드에서 **sysopt connection** 명령을 사용합니다.기본 설정을 복원하려면 이 명령의 no 형식을 사용합니다.기본 최대값은 1380바이트입니다.최소 기능은 기본적으로 비활성화되어 있습니다(0으로 설정).기본 최대 MSS 제한을 변경하려면 다음을 수행합니다.

```
security appliance (config)# sysopt connection tcp-mss MSS_size_in_bytes
```

참고: 최대 크기를 1380보다 크게 설정하면 패킷이 MTU 크기(기본적으로 1500)에 따라 프래그먼트화될 수 있습니다. 프래그먼트가 많으면 Frag Guard 기능을 사용할 때 보안 어플라이언스의 성능에 영향을 줄 수 있습니다.최소 크기를 설정하면 TCP 서버가 클라이언트로 많은 작은 TCP 데이터 패킷을 전송하지 못하게 하고 서버 및 네트워크의 성능에 영향을 줍니다.최소 MSS 제한을 변경하려면 다음을 수행합니다.

```
security appliance (config)# sysopt connection tcp-mss minimum MSS_size_in_bytes
```

보안 어플라이언스(config)# `sysopt tcp-mss MSS_size_in_bytes`**참고:** MPF 컨피그레이션을 참조하여 문서 PIX/ASA 7.X 문제의 MSS 섹션을 초과하는 패킷을 허용하십시오.MSS

Exceeded(MSS 초과됨) - HTTP 클라이언트가 초과된 MSS 패킷을 다른 방법으로 허용하기 위해 일부 웹 사이트에서 자세한 내용을 찾아볼 수 없습니다.

방법 3:경로 MTU 검색(PMTUD)

PMTUD는 프래그먼트화 문제를 해결할 수 있습니다.

TCP MSS의 주요 문제는 관리자가 프래그먼트화가 발생하지 않도록 라우터에서 구성할 값을 알아야 한다는 것입니다.사용자와 원격 VPN 위치 사이에 둘 이상의 경로가 있는 경우 또는 초기 쿼리를 수행할 때 가장 작은 MTU 대신 두 번째 또는 세 번째 작은 MTU가 초기 쿼리 내에서 사용되는 라우팅 결정을 기반으로 하는 경우 문제가 될 수 있습니다.PMTUD를 사용하면 프래그먼트화를 방지하는 IP 패킷의 MTU 값을 결정할 수 있습니다.ICMP 메시지가 라우터에 의해 차단되면 경로 MTU가 끊어지고 DF 비트 집합이 있는 패킷이 삭제됩니다.set **ip df** 명령을 사용하여 DF 비트를 지우고 패킷을 프래그먼트화하고 전송할 수 있습니다.프래그먼트화는 네트워크에서 패킷 포워딩 속도를 늦출 수 있지만 액세스 목록을 사용하여 DF 비트가 지워지는 패킷 수를 제한할 수 있습니다.

1. PMTUD는 다음 세 가지 문제로 인해 작동하지 않을 수 있습니다.중간 라우터는 패킷을 삭제할 수 있으며 ICMP 메시지로 응답하지 않습니다.이는 인터넷에서 매우 흔하지는 않지만 라우터가 ICMP 연결 불가 메시지로 응답하지 않도록 구성된 네트워크 내에서 일반적일 수 있습니다.중간 라우터는 ICMP 연결 불가 메시지로 응답할 수 있지만 반환 흐름에서 방화벽은 이 메시지를 차단합니다.이것은 더 흔한 일이다.ICMP Unreachable 메시지는 소스로 되돌아오지만 소스는 조각화 메시지를 무시합니다.이것은 이 세 가지 문제 중 가장 흔한 것이다.첫 번째 문제가 발생하면 소스가 배치된 IP 헤더의 DF 비트를 지우거나 TCP MSS 크기를 수동으로 조정할 수 있습니다.DF 비트를 지우려면 중간 라우터가 값을 1에서 0으로 변경해야 합니다. 일반적으로 패킷이 네트워크를 나가기 전에 네트워크의 라우터가 이 작업을 수행합니다.이는 IOS 기반 라우터에서 수행하는 간단한 코드 컨피그레이션입니다.

```
Router (config) # access-list ACL_# permit tcp any any
Router (config) # route-map route_map_name permit seq#
Router (config-route-map) # match ip address ACL_#
Router (config-route-map) # set ip df 0
Router (config-route-map) # exit
Router (config) # interface type [slot#/]port #
Router (config-if) # ip policy router-map route_map_name
```

2. **PMTUD 및 GRE 터널**기본적으로 라우터는 자체적으로 생성하는 GRE 터널 패킷에 대해 PMTUD를 수행하지 않습니다.GRE 터널 인터페이스에서 PMTUD를 활성화하고 라우터가 터널을 통과하는 트래픽에 대한 소스/대상 디바이스의 MTU 조정 프로세스에 참여하도록 하려면 다음 컨피그레이션을 사용합니다.라우터(config) # 터널_#라우터(config-if) # `-mtu-discovery`tunnel **path-mtu-discovery** 명령은 라우터의 GRE 터널 인터페이스에 대해 PMTUD를 활성화합니다.선택 사항인 age-timer 매개변수는 터널 인터페이스에서 검색된 최대 MTU 크기를 재설정하는 시간(분)을 지정합니다(GRE 헤더의 경우 24바이트).타이머에 *무한대를* 지정하면 타이머가 사용되지 않습니다.min-mtu 매개 변수는 MTU 값을 구성하는 최소 바이트 수를 지정합니다.
3. **PIX/ASA 7.x - DF(Clear Don't Fragment)** 또는 대용량 파일 또는 패킷을 처리합니다.이 MTU 크기 오류 메시지가 표시되므로 터널을 통해 인터넷, 대용량 파일 또는 애플리케이션에 제대로 액세스할 수 없습니다.

```
PMTU-D packet 1440 bytes greater than effective mtu 1434,
 dest_addr=10.70.25.1, src_addr=10.10.97.55, prot=TCP
```

이 문제를 해결하려면 디바이스의 외부 인터페이스에서 DF 비트를 지워야 합니다.글로벌 컨

피그레이션 모드에서 crypto ipsec df-bit 명령을 사용하여 IPSec 패킷에 대한 DF 비트 정책을 구성합니다.

```
pix(config)# crypto ipsec df-bit clear-df outside
```

IPSec 터널이 포함된 DF 비트 기능을 사용하면 보안 어플라이언스가 캡슐화된 헤더에서 DF(Don't Fragment) 비트를 지우거나 설정하거나 복사할 수 있는지 지정할 수 있습니다.IP 헤더 내의 DF 비트는 디바이스가 패킷을 단편화할 수 있는지 여부를 결정합니다.글로벌 컨피그레이션 모드에서 **crypto ipsec df-bit** 명령을 사용하여 보안 어플라이언스가 캡슐화된 헤더에 DF 비트를 지정하도록 구성합니다.터널 모드 IPSec 트래픽을 캡슐화할 때 DF 비트 clear-df 설정을 사용합니다.이 설정을 사용하면 디바이스에서 사용 가능한 MTU 크기보다 큰 패킷을 전송할 수 있습니다.사용 가능한 MTU 크기를 모르는 경우에도 이 설정이 적합합니다.

참고: 프래그먼트화 문제 및 삭제된 패킷이 여전히 발생하는 경우 선택적으로 ip mtu **tunnel interface** 명령을 사용하여 MTU 크기를 수동으로 조정할 수 있습니다.이 경우 라우터는 패킷을 보호하기 전에 프래그먼트합니다.이 명령은 PMTUD 및/또는 TCP MSS와 함께 사용할 수 있습니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

문제 해결

VPN 암호화 오류

라우터와 PIX 간에 IPSec 터널이 설정되었다고 가정합니다.패킷이 삭제된 암호화 오류 메시지가 표시되면 다음 단계를 완료하여 문제를 해결합니다.

1. 클라이언트에서 서버측으로의 스니퍼 추적을 수행하여 어떤 것이 가장 적합한 MTU인지 확인합니다.ping 테스트를 사용할 수도 있습니다.

   ```
   ping  -l  1400  192.168.1.1 -f
   ```

   192.168.1.1은 원격 시스템의 IP 주소입니다.
2. 응답이 있을 때까지 1400의 값을 20으로 계속 줄입니다.**참고:** 대부분의 경우 작동하는 마법 값은 1300입니다.
3. 적절한 최대 세그먼트 크기를 달성한 후 사용 중인 장치에 맞게 적절히 조정합니다.PIX 방화벽에서:

   ```
   sysopt connection tcpmss 1300
   ```

   라우터에서:

   ```
   ip tcp adjust-mss 1300
   ```

RDP 및 Citrix 문제

문제/장애:

VPN 네트워크 간에 ping할 수 있지만 터널을 통해 RDP(Remote Desktop Protocol) 및 Citrix 연결을 설정할 수 없습니다.

해결책:

문제는 PIX/ASA 뒤의 PC의 MTU 크기가 될 수 있습니다.클라이언트 컴퓨터에 대해 MTU 크기를 1300으로 설정하고 VPN 터널 전체에서 Citrix 연결을 설정해 보십시오.

관련 정보

- GRE 및 IPSEC의 IP 프래그먼트화, MTU, MSS 및 PMTUD 문제 해결
- PIX/ASA 7.0 문제:MSS 초과 - HTTP 클라이언트가 일부 웹 사이트를 검색할 수 없음
- 가장 일반적인 L2L 및 원격 액세스 IPSec VPN 문제 해결 솔루션
- GRE 터널을 사용할 때 인터넷을 탐색할 수 없는 이유
- 기술 지원 및 문서 – Cisco Systems