

### Configurable MTU and TCP MSS clamping

---

#### Contents

Contents .....	1
Overview .....	1
MTU discovery .....	2
MSS clamping .....	4
MTU and VPN .....	5
Configurable MTU and MSS clamping on Contivity .....	6
MTU on Contivity .....	7
TCP MSS clamping on Contivity .....	9
DF bit on Contivity .....	9
Configuring MTU, MSS and DF bit .....	9
Configuring MTU, MSS and DF bit via GUI .....	10
Configuring MTU on LAN interfaces .....	10
Configuring TCP MSS on LAN interface .....	12
Configuring TCP MSS on PPPoE interface .....	14
Configuring MTU and TCP MSS for the Dial Interface .....	16
Configuring MTU and TCP MSS on WAN interface .....	17
Configuring MTU for the tunnel .....	17
Configuring DF bit for the IPSec tunnels .....	19
Configuring MTU and MSS via CLI .....	22
Event Log messages .....	28
Sample Configurations .....	29
Tunnel MTU .....	29
Setup .....	29
Configuring WS1 .....	29
Configuring WS2 .....	30
Configuring CES1 .....	30
Configuring CES2 .....	38
Testing configuration .....	46
TCP MSS Clamping .....	49
Setup .....	49
Configuring WS .....	49
Configuring CES .....	50
Configuring FTPS .....	54
Testing configuration .....	55

#### Overview

The Internet is a world-wide network that provides connection between computers via telecommunication links and enables computers to communicate with each other. The Internet is not a homogeneous network but rather a collection of interconnected networks. Each of the networks may be built on different network elements and technologies and therefore have different characteristics in terms of speed, throughput and bandwidth. For example, some of the networks might use PPPoE (Point-to-Point Protocol over Ethernet), others Ethernet, and some might use Frame Relay or ATM as their connection.

Each technology used in the network has a different largest packet or datagram size it can transmit without it needing to break it down (or fragment) into smaller units. This largest

### Configurable MTU and TCP MSS clamping

---

size in bytes is known as Maximum Transmission Unit, or MTU. For example, the typical MTU value for the Ethernet is 1500 bytes, 1492 bytes for PPPoE, 4352 bytes for the FDDI or 4464 for 4Mbps Token Ring. The default value of the network MTU may be overridden by the administrator due to, for example, local network needs.

Larger and more consistent MTUs throughout the network may reduce or eliminate the fragmentation and thus enhance performance. Larger MTU increase systems performance by minimizing the number of packets processed, as most of the performance costs is in “packets handled” rather than “bytes transferred”. On the other hand, for dial-up connections it’s better to keep the MTU smaller, to maintain good interactive response. Thus care must be taken when choosing MTU values for the network, to accommodate the needs of users, and maintain the performance of the network.

### MTU discovery

Systems on the network have no knowledge of the MTU values used for each network or peer systems. A mechanism called path MTU discovery is used to find out MTU parameters in other networks.

Consider the situation depicted on Figure 1, Host A has a large amount of data to send to Host B and the path to Host B lies through a number of networks with different MTU values, so that  $MTU\ 4 > MTU\ 1 > MTU\ 2 > MTU\ 3$ . What MTU should be used to send the data to Host B?

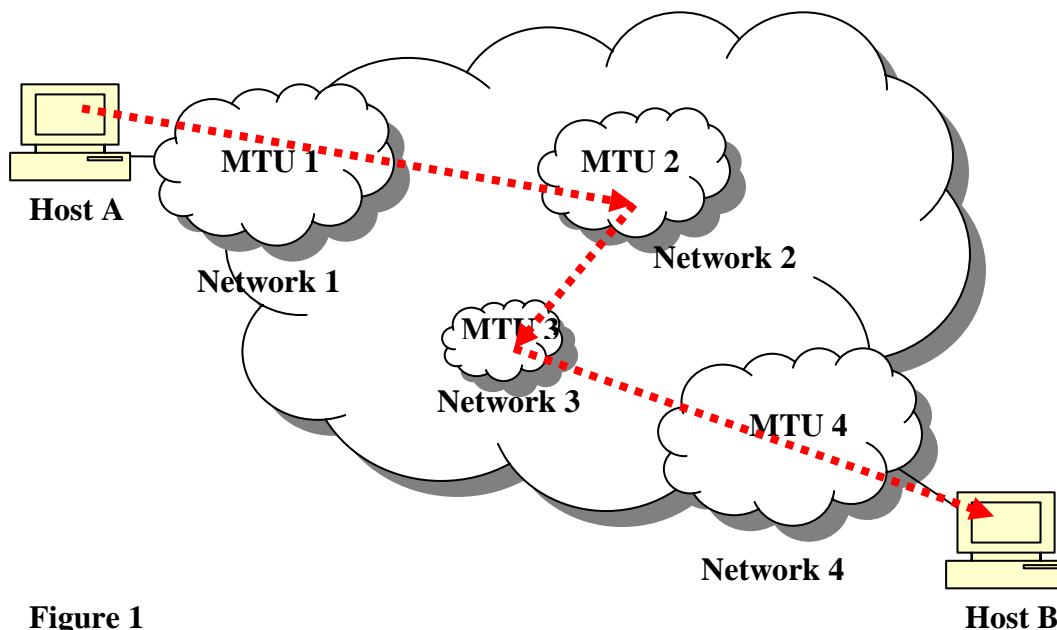


Figure 1

### Configurable MTU and TCP MSS clamping

---

Without having any knowledge of MTU across the network Host A initially assumes that MTU throughout the path is equal to the MTU of its first hop, or MTU 1. So Host A starts to send the data using the MTU 1 and the Don't Fragment (DF) bit set.

Along the way the datagram reaches some router in Network 2. The router notices that the received data has a larger MTU than the second network can transmit, and with DF bit being set, the router in Network 2 discards the datagram. The router returns an ICMP Destination Unreachable message with a code meaning "fragmentation needed and DF bit set" back to Host A. Some routers specify the correct value for the MTU in its network in the ICMP message, so the source does not have to guess the value.

Upon receipt of this message Host A reduces its assumed MTU for that path and tries to send the datagram again. If the second attempt is successful and the selected MTU is less or equal to the MTU 2, the router in the second network processes the packets and sends it along the way to Network 3. If not, the process starts again until Host A sends the correct size.

Once the datagram reaches Network 3 the same process of MTU discovery repeats. With MTU 2 being larger than MTU 3, the router in Network 3 discards the datagram and responds with an ICMP Destination Unreachable message to Host A. Host A adjusts MTU until the router in Network 3 agrees to process the packet, thus setting MTU to MTU 3.

When the datagram reaches Network 4, MTU is equivalent to MTU 3 which is smaller than MTU 4, so the datagram is processed and is sent to Host B.

Thus, at the end Host A has learned the path MTU (the smallest MTU used along the path – MTU 3) and will use that value to send the data to Host B.

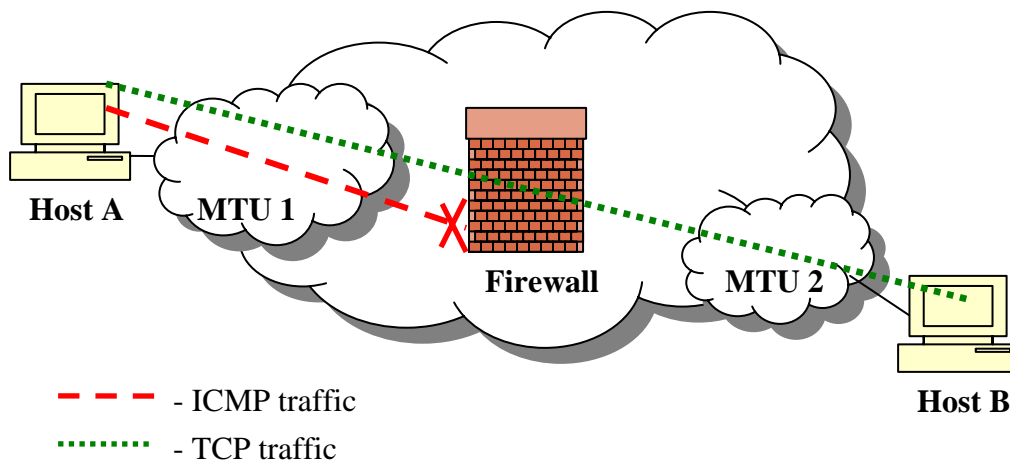
For more information on path MTU discovery please consult:  
RFC 1191 <http://www.ietf.org/rfc/rfc1191.txt>

### Configurable MTU and TCP MSS clamping

---

#### MSS clamping

Some routers along the way might fail to respond with the ICMP Destination Unreachable messages for a variety of reasons ranging from router software bugs to configuration problems. Firewalls are often misconfigured to suppress all ICMP to messages (Figure 2) (refer to RFC 1435 <http://www.ietf.org/rfc/rfc1435.txt> and RFC 2923 <http://www.ietf.org/rfc/rfc2923.txt>). This would cause MTU discovery process to fail, as ICMP messages will not be received by the originating host. Upper layer protocols will continue to send large packets without discovering that they need to reduce the packets size. This might lead upper layer protocols, like TCP, to fail as the connection will eventually time out.



**Figure 2**

The solution to this problem is to use the TCP Maximum Segment Size (MSS) option. This option may be used at the time a connection is established (only) to indicate the maximum size TCP segment that can be accepted on that connection. This Maximum Segment Size announcement is sent from the data receiver to the data sender and says "I can accept TCP segments up to size X". The size (X) may be larger or smaller than the default. The process of setting the maximum packet size through the MSS option is known as MSS clamping. With MSS option being part of TCP no ICMP traffic is needed to adjust the MTU values between peers. The MSS can be used completely independently in each direction of data flow, as a result there can be different maximum sizes in two directions.

MSS counts only data bytes; it does not count TCP or IP headers. Therefore the value for the MSS can be calculated as:

$$\text{MSS} = \text{MTU} - \text{sizeof}(\text{TCP header}) - \text{sizeof}(\text{IP header})$$

### Configurable MTU and TCP MSS clamping

---

Usually a best case scenario is assumed where TCP and IP headers have minimum size of 20 bytes each; this gives a modified formula for calculating the MSS:

$$\text{MSS} = \text{MTU} - 40$$

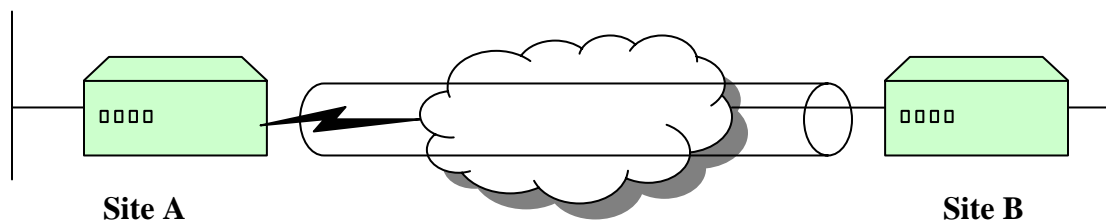
So if MTU for Ethernet is 1500 bytes, the MSS option would be 1460 bytes.

For more information on TCP MSS option please consult:

RFC 879 <http://www.ietf.org/rfc/rfc1191.txt>

### MTU and VPN

Consider a situation when two sites are connected via VPN tunnel and one of the sites uses PPPoE interface as its connection to the Internet (Figure 3).



**Figure 3**

If tunnel MTU is larger than the PPPoE MTU of the interface, then fragmentation is required. If the DF (don't fragment) bit is set or the ISP (Internet Service Provider) that provides the PPPoE service for Site A does not support fragmentation for PPPoE circuits, the packets will be dropped as they will be larger than the underlying PPPoE can carry. As a result there is a need to have the ability to configure MTU for the tunnels and to set or clear the DF bit.

### Configurable MTU and TCP MSS clamping

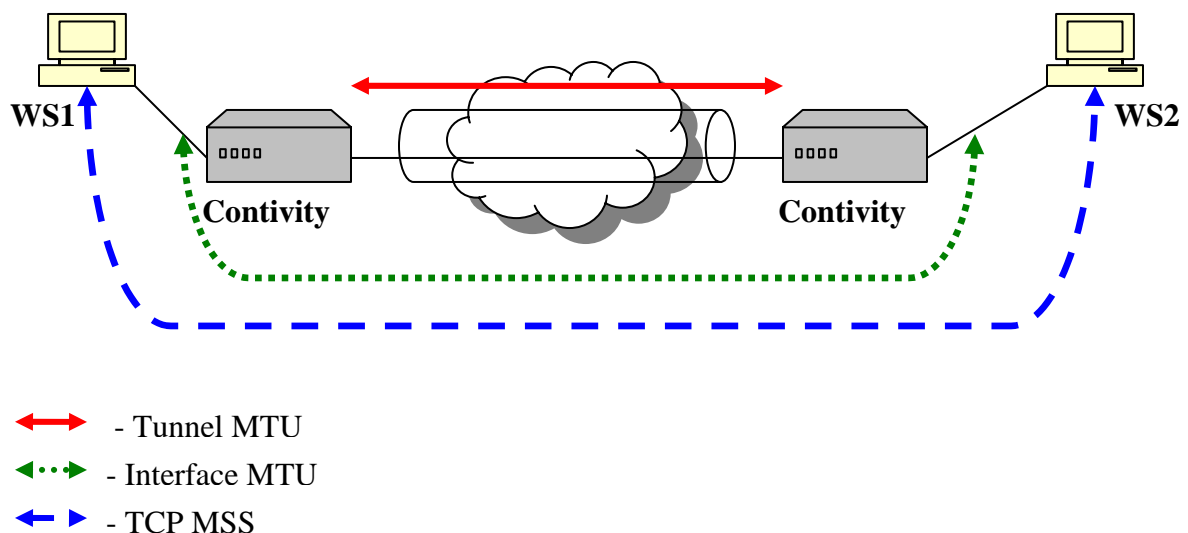
---

#### Configurable MTU and MSS clamping on Contivity

Code release V04\_85 (V04\_90) allows Contivity Secure IP Services Gateway to control packet fragmentation through:

- Interface MTU configuration;
- Tunnel MTU configuration;
- TCP MSS clamping;
- IPSec DF bit behavior configuration.

Contivity allows MTU values to be configured for each of its physical and tunnel interfaces. Furthermore, the TCP MSS option (MSS clamping) can be enabled and configured on physical interfaces (Figure 4).



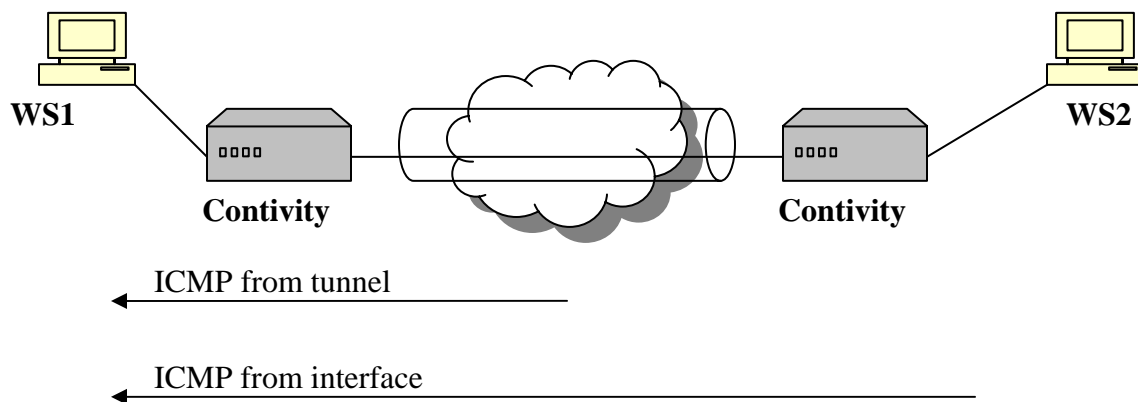
**Figure 4**

### Configurable MTU and TCP MSS clamping

---

#### MTU on Contivity

Consider the situation depicted in Figure 5. WS1 sends initial data to WS2 with DF bit set and WS1's assumption of the MTU used throughout the network. If fragmentation is required at the tunnel or interface, an ICMP message is sent back to WS1. WS1 adjusts the size of the packets sent and the transfer continues.



**Figure 5**

Contivity has the ability to configure MTU on a per interface basis. The default MTU value of all physical interfaces is 1500 to maintain backward compatibility with existing configurations. The maximum MTU value allowed to be assigned to an interface varies based on the media used for the interface and layer 2 encapsulation. Thus Contivity accepts the following maximum configurable MTU values:

- Ethernet 1500,
- PPPoE 1492,
- WAN link 1788,
- Serial 1788.

Value 1788 is derived from the maximum buffer size Contivity can hold. The minimum MTU is 576.

### Configurable MTU and TCP MSS clamping

---

In addition Contivity has the ability to configure MTU on tunnels. This value is configured per connection, so different tunnels may have different MTU settings.

If MTU is not configured for the tunnel then the largest payload that goes into a tunnel without fragmentation (effective tunnel MTU) is derived from interface MTU and layer 3 encapsulation (Table 1):

Tunnel Type	Derived Effective Tunnel MTU
IPSec	Interface MTU - 56
PPTP	Interface MTU - 32
L2TP	Interface MTU - 40
L2TP over IPSec	Interface MTU - 72
L2F	Interface MTU - 40

**Table 1**

If MTU is configured for the tunnel the largest payload is derived from configured MTU.

**Note:** MTU is a property of a physical interface. CLIP (Circuit Less IP) is associated with the box and uses the loopback interface, which has MTU of 1500. CLIP/loopback MTU is not configurable.

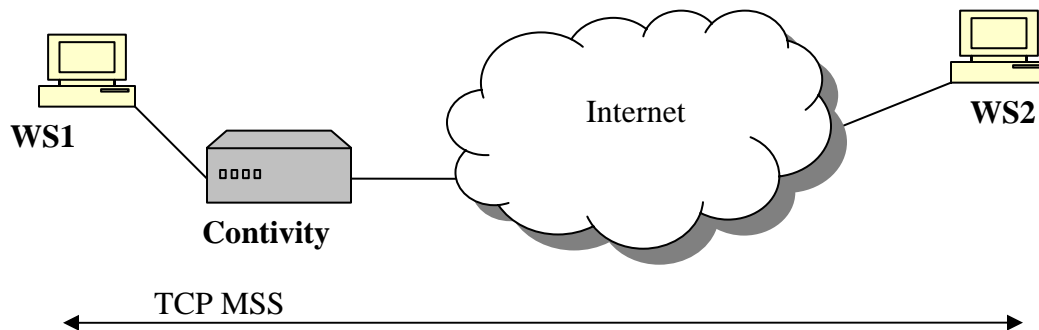


### Configurable MTU and TCP MSS clamping

---

#### TCP MSS clamping on Contivity

Consider the situation depicted in Figure 6. Suppose there is an issue with the MTU discovery somewhere in the Internet along the way from WS1 to WS2. If TCP MSS option is set on the Contivity interface, that value will be used to calculate the packet size to be sent and TCP peers WS1 and WS2 will not send packets larger than the configured value.



**Figure 6**

TCP MSS clamping applies to packets that transit Contivity gateway and to packets that originate or end on Contivity. TCP clamping is done on clear text packets; once packets are encrypted the contents cannot be modified. The default value for TCP MSS is calculated as configured MTU minus 40. TCP MSS clamping is disabled by default.

#### DF bit on Contivity

The new version of Contivity code allows administrator to set, copy or clear DF bit for IPSec tunnels. Based on the configuration the DF bit in the outer header is set, cleared or copied from inner header.

When a packet with the DF-bit set is received by the Contivity and the packet requires fragmentation, Contivity will drop the packet and return the ICMP error message to the originator. If an IPSec packet has the DF-bit set in the outer header, Contivity will be unable to return ICMP error message to the originator.

The DF bit is configured on tunnels at the group level, so if several tunnels belong to the same group all of them will inherit the DF bit functionality.

### Configuring MTU, MSS and DF bit

The configuration of MTU and MSS can be done via GUI or CLI.

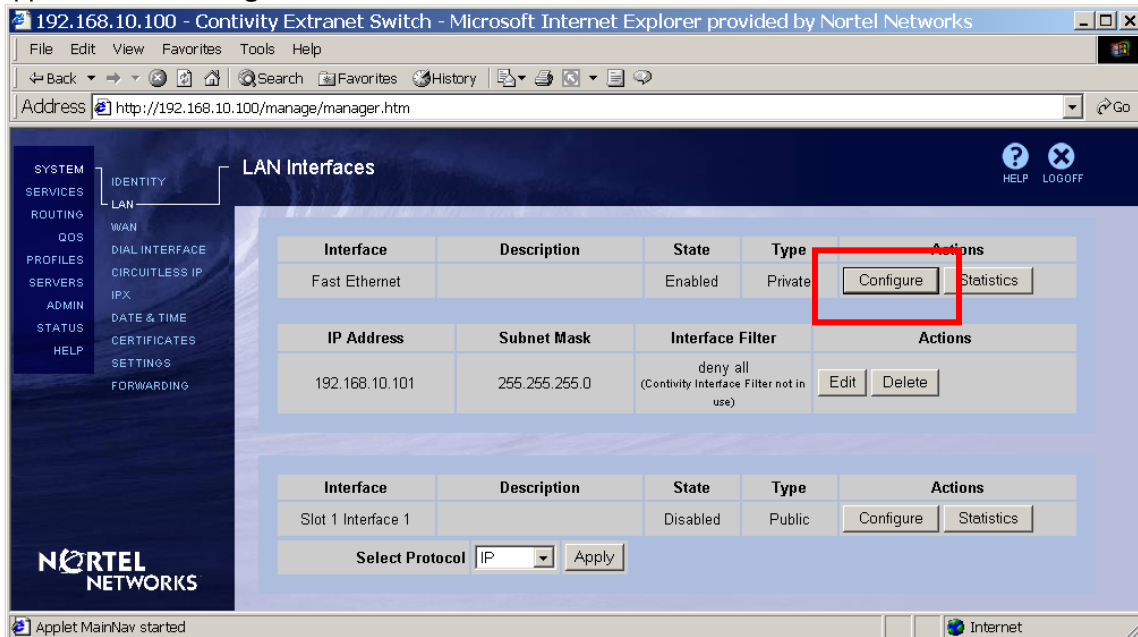
### Configurable MTU and TCP MSS clamping

## Configuring MTU, MSS and DF bit via GUI

**NOTE:** Changing MTU and/or MSS values on interfaces and tunnels will cause interfaces and tunnels to bounce. Changing DF bit setting will cause all tunnels in the group to bounce.

### Configuring MTU on LAN interfaces

Navigate **System**→**LAN** to configure MTU for LAN interfaces. The **LAN Interfaces** screen appears. Click **Configure** next to the selected interface:



The screenshot shows the 'LAN Interfaces' configuration page in a web browser. The browser's address bar shows 'http://192.168.10.100/manage/manager.htm'. The page has a dark blue sidebar with a navigation menu. The main content area is titled 'LAN Interfaces' and contains two tables. The first table lists interfaces, with 'Fast Ethernet' selected. The 'Configure' button for this interface is highlighted with a red box. The second table shows the configuration for the selected interface, including IP address, subnet mask, and interface filter. Below the tables, there is a 'Select Protocol' dropdown menu set to 'IP' and an 'Apply' button.

Interface	Description	State	Type	Actions
Fast Ethernet		Enabled	Private	<a href="#">Configure</a> <a href="#">Statistics</a>

IP Address	Subnet Mask	Interface Filter	Actions
192.168.10.101	255.255.255.0	deny all (Contivity Interface Filter not in use)	<a href="#">Edit</a> <a href="#">Delete</a>

Interface	Description	State	Type	Actions
Slot 1 Interface 1		Disabled	Public	<a href="#">Configure</a> <a href="#">Statistics</a>

Select Protocol:  [Apply](#)

# Configuration Guide

## Contivity Secure IP Services Gateway



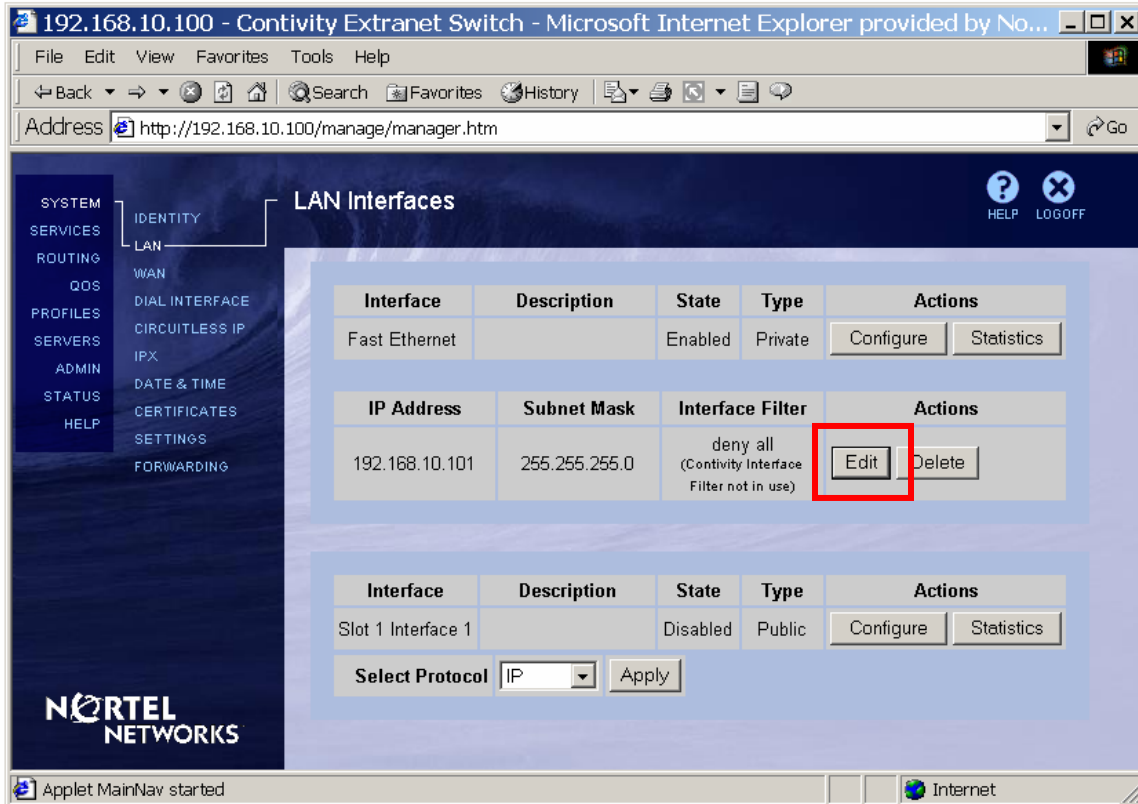
### Configurable MTU and TCP MSS clamping

The **LAN Interfaces→Edit LAN Interface** screen appears. Enter the **MTU** value (between 576 and 1500 for Ethernet) to be used for the interface (1500 is the default value for the Ethernet) and click **OK**:

### Configurable MTU and TCP MSS clamping

#### Configuring TCP MSS on LAN interface

Navigate **System**→**LAN** to configure TCP MSS option for the LAN interface. Click **Edit** next to the interface to be configured:



The screenshot shows a web browser window titled "192.168.10.100 - Contivity Extranet Switch - Microsoft Internet Explorer provided by No...". The address bar shows "http://192.168.10.100/manage/manager.htm". The interface has a dark blue sidebar with a menu: SYSTEM, SERVICES, ROUTING, QOS, PROFILES, SERVERS, ADMIN, STATUS, and HELP. The main content area is titled "LAN Interfaces" and contains two tables. The first table lists interfaces: "Fast Ethernet" (Enabled, Private) with "Configure" and "Statistics" buttons. The second table lists IP addresses: "192.168.10.101" (Subnet Mask: 255.255.255.0, Interface Filter: deny all) with "Edit" and "Delete" buttons. The "Edit" button is highlighted with a red rectangle. Below the tables is a "Select Protocol" dropdown menu set to "IP" and an "Apply" button. The Nortel Networks logo is in the bottom left corner of the interface.

Interface	Description	State	Type	Actions
Fast Ethernet		Enabled	Private	Configure Statistics

IP Address	Subnet Mask	Interface Filter	Actions
192.168.10.101	255.255.255.0	deny all (Contivity Interface Filter not in use)	Edit Delete

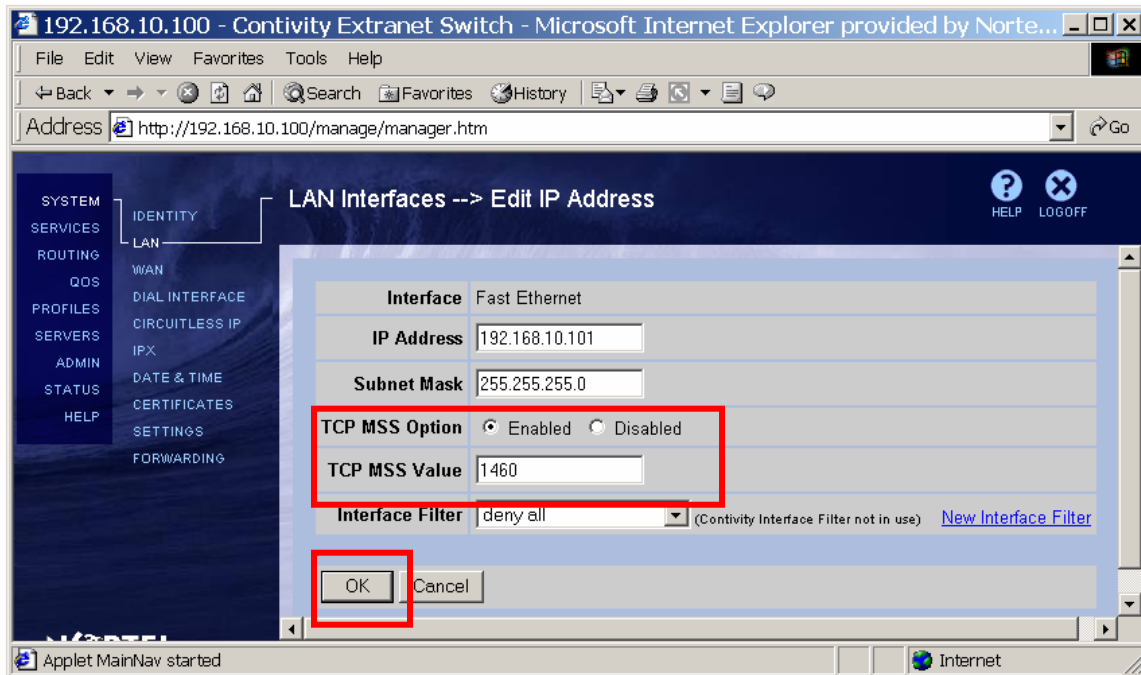
Interface	Description	State	Type	Actions
Slot 1 Interface 1		Disabled	Public	Configure Statistics

Select Protocol: IP Apply

### Configurable MTU and TCP MSS clamping

The **LAN Interfaces→Edit IP Address** screen appears.

Select **Enabled** next to **TCP MSS Option** parameter to enable TCP MSS. Enter the **TCP MSS Value** to be used for the interface (1460 by default for Ethernet, MTU 1500 minus 40) and click **OK**:



192.168.10.100 - Contivity Extranet Switch - Microsoft Internet Explorer provided by Norte...

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History

Address http://192.168.10.100/manage/manager.htm Go

SYSTEM SERVICES ROUTING QOS PROFILES SERVERS ADMIN STATUS HELP

IDENTITY LAN WAN DIAL INTERFACE CIRCUITLESS IP IPX DATE & TIME CERTIFICATES SETTINGS FORWARDING

LAN Interfaces --> Edit IP Address

Interface Fast Ethernet

IP Address 192.168.10.101

Subnet Mask 255.255.255.0

TCP MSS Option ☒ Enabled ☐ Disabled

TCP MSS Value 1460

Interface Filter deny all (Contivity Interface Filter not in use) [New Interface Filter](#)

OK Cancel

Applet MainNav started Internet

# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

#### Configuring TCP MSS on PPPoE interface

Navigate **System**→**LAN**. Click **Edit** next to the PPPoE interface:

192.168.10.100 - Contivity Extranet Switch - Microsoft Internet Explorer provided by Nortel Networks

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites History Print

Address <http://192.168.10.100/manage/manager.htm> Go

SYSTEM  
SERVICES  
ROUTING  
QOS  
PROFILES  
SERVERS  
ADMIN  
STATUS  
HELP

IDENTITY  
LAN  
WAN  
DIAL INTERFACE  
CIRCUITLESS IP  
IPX  
DATE & TIME  
CERTIFICATES  
SETTINGS  
FORWARDING

LAN Interfaces

HELP LOGOFF

Interface	Description	State	Type	Actions
Fast Ethernet		Enabled	Private	Configure Statistics

IP Address	Subnet Mask	Interface Filter	Actions
192.168.10.101	255.255.255.0	deny all (Contivity Interface Filter not in use)	Edit Delete

Interface	Description	State	Type	Actions
Slot 1 Interface 1		Disabled	Public	Configure Statistics

Local IP Address	Interface Protocol	Administrative State	Operational State	Interface Filter	Actions
0.0.0.0 (Dynamic)	PPPoE	Disabled	Down	deny all (Default Filter) (Contivity Interface Filter not in use)	Edit Delete

NORTEL NETWORKS

Applet MainNav started

Internet

# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

The **LAN Interfaces→Edit PPPoE Interface** screen appears.

Select **Enabled** for the **TCP MSS Option** parameter.

Enter the **TCP MSS Value** to be used for that PPPoE interface (1452 by default) and click **OK**:

# Configuration Guide

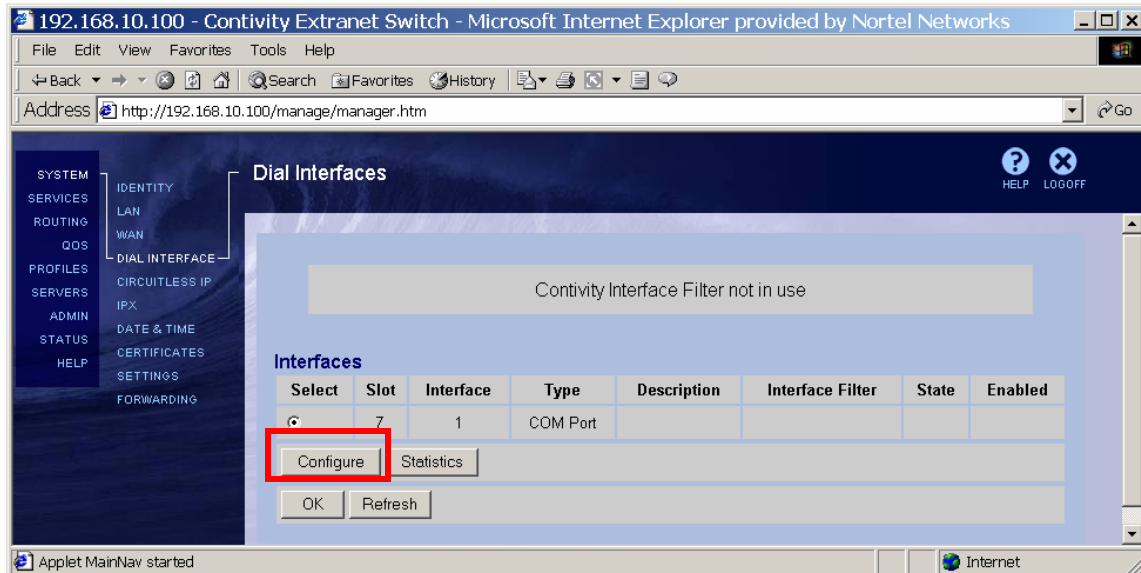
## Contivity Secure IP Services Gateway



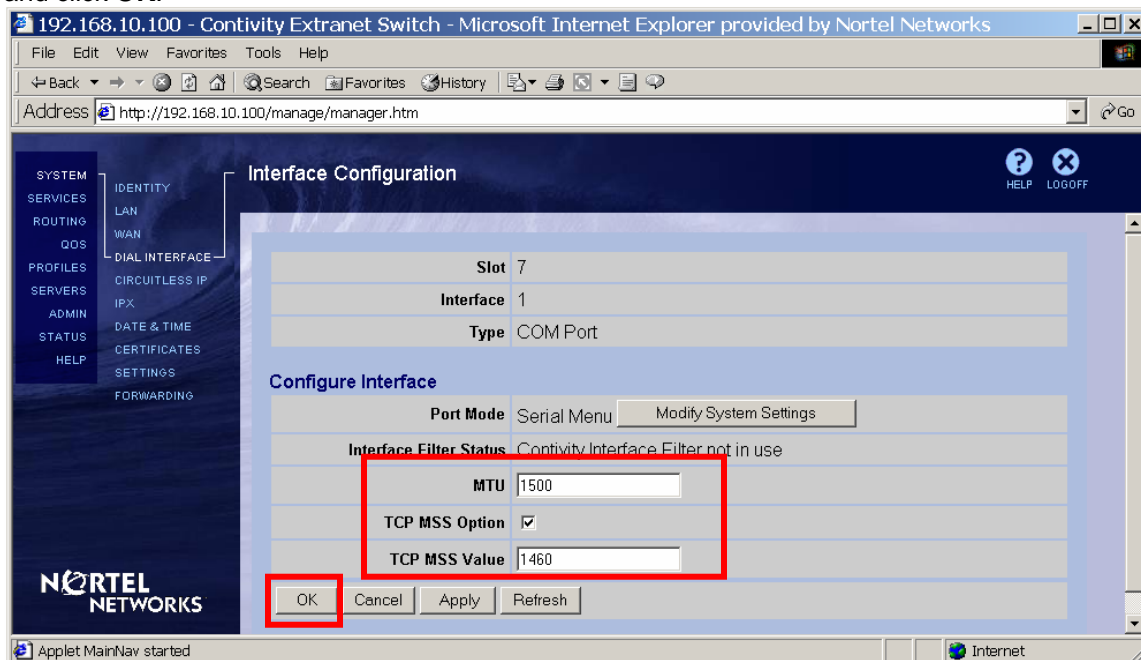
### Configurable MTU and TCP MSS clamping

#### Configuring MTU and TCP MSS for the Dial Interface

Navigate **System**→**Dial Interface**. The Dial Interface screen appears. Select the interface to be configured and click **Configure**:



The **Interface Configuration** screen appears. Enter the **MTU** to be used for the interface (the default is 1500) enter the value between 576 and 1724. Check the box next to **TCP MSS Option** to enable TCP MSS if MSS is required for the setup. Enter the **TCP MSS Value** (default 1460) and click **OK**:





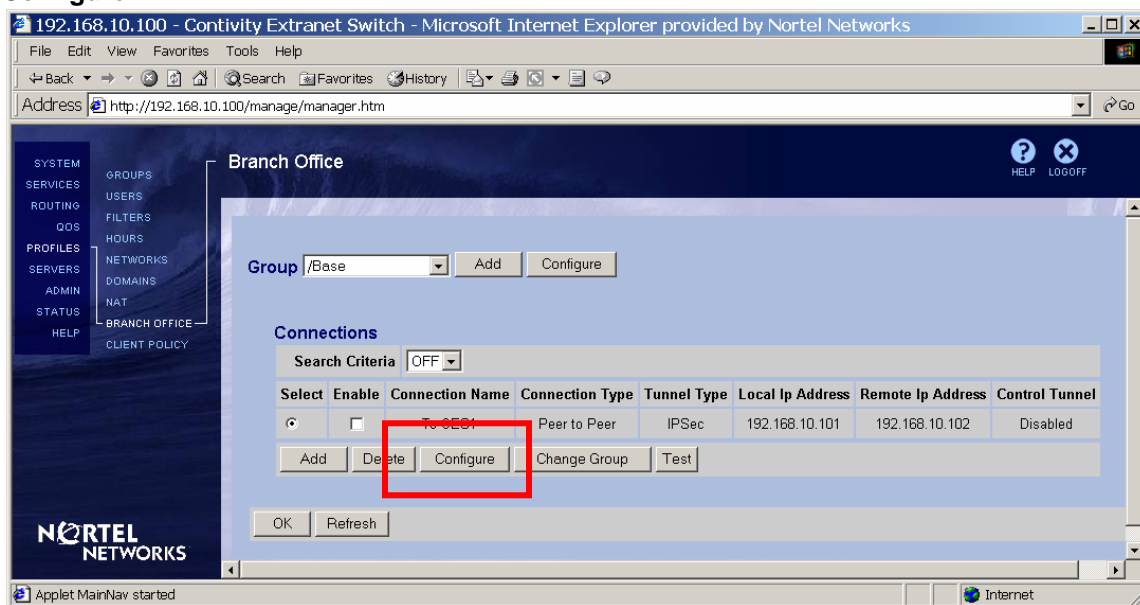
### Configurable MTU and TCP MSS clamping

#### Configuring MTU and TCP MSS on WAN interface

Navigate **System**→**WAN**. The rest of the configuration is done in the same manner as for Dial Interface. Select the dial interface, click **Configure**, enable the TCP MSS option and set the value.

#### Configuring MTU for the tunnel

Navigate **Profiles**→**Branch Office**. Select the branch office interface to be configured and click **Configure**:



# Configuration Guide

## Contivity Secure IP Services Gateway



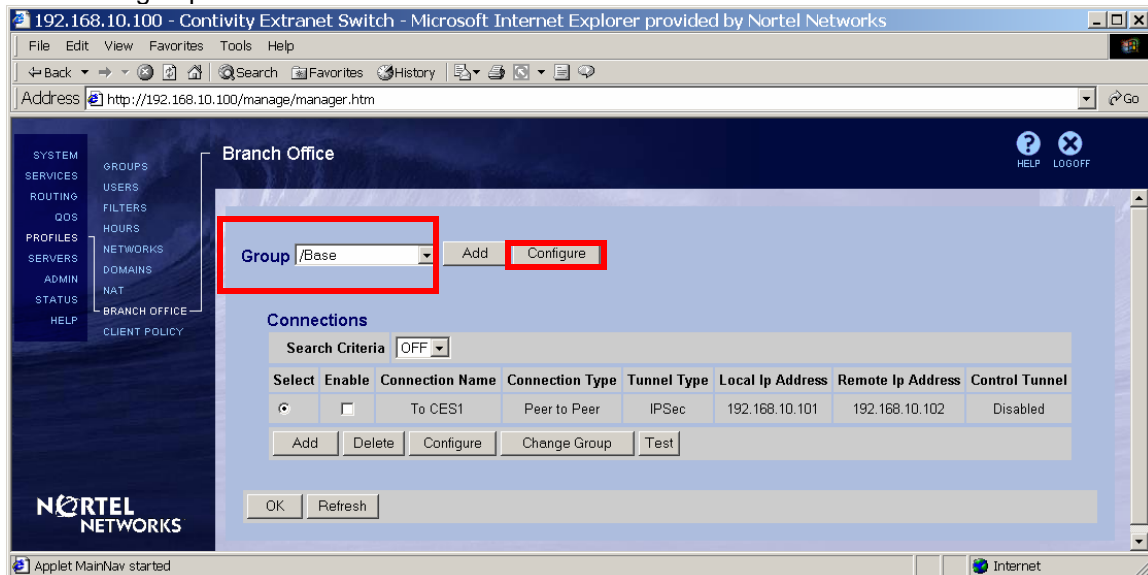
### Configurable MTU and TCP MSS clamping

The **Connection Configuration** screen appears. Scroll down to the **MTU** section. Select whether **MTU** should be **Enabled** from the drop down list. Set the **MTU Value** to be used (the default is set to 1788). Click **OK** at the bottom of the screen:

### Configurable MTU and TCP MSS clamping

#### Configuring DF bit for the IPSec tunnels

Navigate **Profiles**→**Branch Office**. Select the **Group** the tunnel belongs to and click **Configure** next to the group:



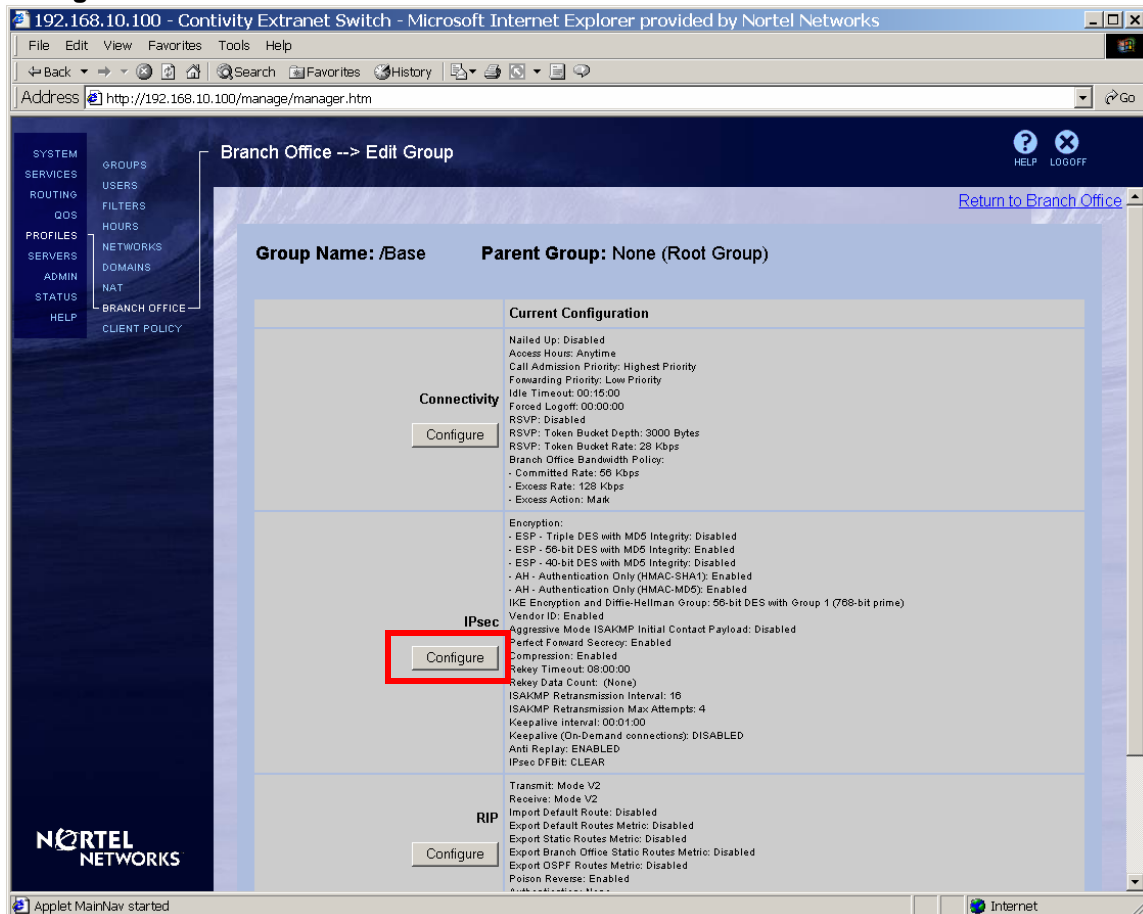
# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

The **Branch Office→Edit Group** screen appears. Scroll down to **IPSec** section and click **Configure**:



# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

Select the DF bit setting from the drop down list next to **IPSec DF Bit**:

**Clear** - default, sets the DF bit in the outer header to 0;

**Copy** - copies DF bit for the from the inner header;

**Set** - set DF bit the outer header to 1.

Click **OK**:

192.168.10.100 - Contivity Extranet Switch - Microsoft Internet Explorer provided by Nortel Networks

Address: http://192.168.10.100/manager/manager.htm

Branch Office

Group Name: /Base

Field	Value
Encryption	ESP - Triple DES with MD5 Integrity <input type="checkbox"/>
	ESP - 56-bit DES with MD5 Integrity <input checked="" type="checkbox"/>
	ESP - 40-bit DES with MD5 Integrity <input type="checkbox"/>
	AH - Authentication Only (HMAC-SHA1) <input checked="" type="checkbox"/>
	AH - Authentication Only (HMAC-MD5) <input checked="" type="checkbox"/>
IKE Encryption and Diffie-Hellman Group	56-bit DES with Group 1 (768-bit prime)
Vendor ID	Enabled
Aggressive Mode ISAKMP Initial Contact Payload	Disabled
Perfect Forward Secrecy	Enabled
Compression	Enabled
Rekey Timeout	08:00:00
Rekey Data Count	0 Kb
ISAKMP Retransmission Interval	16
ISAKMP Retransmission Max Attempts	4 (Range 0 - 10)
Keepalive interval	00:01:00
Keepalive (On-Demand connections)	Disabled
Anti Rekey	Enabled
IPsec DFBit	Clear

OK Cancel

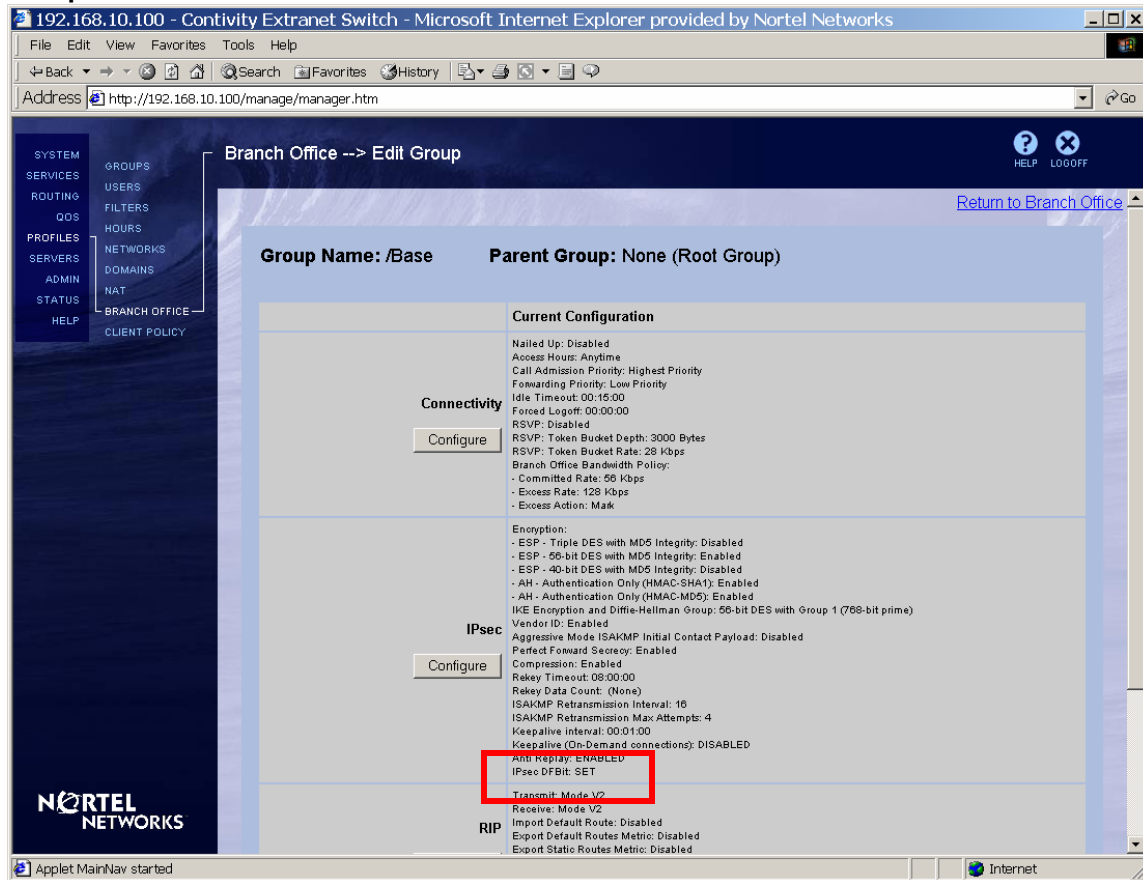
# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

The configured value is listed next to **IPsec DF Bit** parameter on the **Branch Office→Edit Group** screen:



### Configuring MTU and MSS via CLI

To configure Contivity using CLI you need to either telnet to Contivity or connect to it through the serial interface -> option "L" on the menu.

Enter the privileged mode:

```
CES>enable
Password:
```

Enter configuration mode:

```
CES#configure terminal
Enter configuration commands, one per line. End with Ctrl/z.
CES(config)#
```

### Configurable MTU and TCP MSS clamping

---

To view the choice of interfaces:

```
CES(config)#interface ?
Selects an interface to configure OR configures an interface group
  bri           Configures a BRI (ISDN) Interface
  dial          Configures a dial interface
  FastEthernet  FastEthernet IEEE 802.3
  GigabitEthernet Gigabit Ethernet IEEE 802.3ab
  group         Creates or configures an interface group
  serial        Configures a serial interface
```

To enter the interface configuration mode for the FastEthernet 0/1 (private LAN interface):

```
CES(config)#interface FastEthernet 0/1
CES(config-if)#
```

To set the MTU to 1400 for the FastEthernet:

```
CES(config-if)#mtu 1400
```

To enable TCP MSS option for the interface:

```
CES(config-if)#tcp-mss enable
```

To set the TCP MSS option to 1360:

```
CES(config-if)#tcp-mss 1360
```

To exit the interface configuration mode:

```
CES(config-if)#exit
CES(config)#
```

To enter the configuration mode for dial interface on slot 7/port 1:

```
CES(config)#interface dial 7/1
CES(config-if)#
```

To set MTU to 1720:

```
CES(config-if)#mtu 1720
```

To exit the interface configuration mode:

```
CES(config-if)#exit
CES(config)#
```

To enter IPsec configuration mode for the group (/Base):

```
CES(config)#bo-group ipsec "/Base"
CES(config-bo_group/ipsec)#
```

To view configuration options for the DF bit:

```
CES(config-bo_group/ipsec)#df-bit ?
CLEAR  Clears the DF-bit in the outer header.
```

### Configurable MTU and TCP MSS clamping

---

COPY	Copies the DF-bit from the inner header to the outer.
SET	Sets the DF-bit in the outer header.

To set DF bit to Copy:

```
CES(config-bo_group/ipsec)#df-bit COPY
```

To exit IPsec BO group configuration mode:

```
CES(config-bo_group/ipsec)#exit  
CES(config)#
```

To enter branch office configuration mode for connection named "To CES1" of group /Base:

```
CES(config)#bo-conn "To CES1" "/Base"  
CES(config/bo_conn)#
```

To enable MTU for the branch office tunnel:

```
CES(config/bo_conn)#mtu enable
```

To set MTU for the tunnel to 1700:

```
CES(config/bo_conn)#mtu 1700
```

To exit branch office configuration mode:

```
CES(config/bo_conn)#exit  
CES(config)#
```



### Configurable MTU and TCP MSS clamping

---

To view configuration for the branch office named "To CES" of group "/Base":

```
CES(config)#show bo-conn "To CES1" "/"Base"
General Settings:
  State                               : Disabled
  Connection Type                     : Peer-to-Peer
  Tunnel Type                         : IPSec
  Local End Point                     : 192.168.10.101
  Remote End Point                    : 192.168.10.102
  Filter                             : permit all
  Routing Type                       : Static
  Nat                                 : Not Configured
  Local Gateway                       : 0
  MTU Enabled                         : Enabled
  MTU                                 : 1700

Static Routing Settings:
  Local Network                       : Net 20
  192.168.20.0-255.255.255.0
  Remote Network                     State      Cost
  -----
  192.168.10.0-255.255.255.0      Enabled   10

Dynamic Routing Settings:
  RIP State                          : Enabled
  RIP Cost                           : 1
  OSPF State                         : Disabled
  OSPF Area ID                       : 0.0.0.0
  OSPF Cost                          : 100

IPSec Settings:
  Initiator ID                       : Not Configured
  Authentication Type                : Text
  Text Password                      : *****
  Hex Password                       : Not Configured
  Subject DN Type                    : Not Configured
  Subject Common Name                : Not Configured
  Subject Country                    : Not Configured
  Subject Locality                   : Not Configured
  Subject State                     : Not Configured
  Subject Email                     : Not Configured
  Subject Organization               : Not Configured
  Subject Organizational Unit        : Not Configured
```

### Configurable MTU and TCP MSS clamping

---

To view IPsec DF bit group settings for the “/Base” group:

```
CES(config)#show bo-group ipsec "/Base"
Ipssec Settings:
  Rekey Timeout                               : 08:00:00
  Rekey Data Count                           : 0
  Perfect Forward Secrecy                    : Enabled
  Compression                                : Enabled
  ESP - AES 128 with SHA1 Integrity           : Disabled
  ESP - Triple DES with SHA1 Integrity        : Disabled
  ESP - Triple DES with MD5 Integrity         : Disabled
  ESP - 56-bit DES with SHA1 Integrity        : Disabled
  ESP - 56-bit DES with MD5 Integrity        : Enabled
  ESP - 40-bit DES with SHA1 Integrity        : Disabled
  ESP - 40-bit DES with MD5 Integrity        : Disabled
  ESP - NULL (Authentication Only) with SHA1 Integrity : Disabled
  ESP - NULL (Authentication Only) with MD5 Integrity : Disabled
  AH - Authentication Only (HMAC-SHA1)       : Enabled
  AH - Authentication Only (HMAC-MD5)       : Enabled
  IKE Encryption and Diffie-Hellman Group    : des56-group1
  Aggressive Mode ISAKMP Initial Contact Payload Accept : Disabled
  Vendor Id                                  : Enabled
  ISAKMP Retransmission Interval             : 16
  ISAKMP Retransmission Max Attempts         : 4
  Keepalive Interval                         : 00:01:00
  Keepalive On Demand Connections           : Disabled
  Anti Replay                               : Enabled
  DF Bit                                   : COPY
```

To exit configuration mode:

```
CES(config)#exit
CES#
```

# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

---

To view TCP MSS settings for private LAN on slot 0/port 1:

```
CES#show interface FastEthernet 0/1
FastEthernet Interface 0/1 Configuration
  Description          :
  DHCP-relay           : Disabled
  Duplex               : AutoNegotiate
  Filter               : deny all
  IP Address           : 192.168.10.101
  Mac pause            : Disabled
  MTU                  : 1400
  PPPoE                : Disabled
  Public/Private       : Private
  DHCP Service         : Disabled
  Status               : Enabled
  Speed                : AutoNegotiate
TCP-Maximum Segment Size Clamping: Enabled
TCP-Maximum Segment Size [bytes]: 1360
```

To view dial interface settings on slot 7/port 1:

```
CES#show interface dial 7/1
Interface Dial 7/1
  Menu Access Level    : UNRESTRICTED
  Auto answer          : 1 ring
  Baud Rate             : 9600
  Circuit ID           :
  Description           :
  Dial Prefix String    : +++ATDT
  Filter               : deny all
  Modem Command String  :
  Modem Init String     : +++ATZ
  Modem Termination String : +++ATH
  MTU                   : 1720
  Phone                 :
  Mode                  : Serial Menu
  Connection Status     : Used for Serial Menu
  Serial Interface Type : SerialUart
TCP-Maximum Segment Size Clamping : Enabled
TCP-Maximum Segment Size [bytes] : 1460
```

### Configurable MTU and TCP MSS clamping

---

#### Event Log messages

##### **MTU for LAN interface has been changed from 1500 to 1490:**

01/16/2004 08:45:22 0 tHttpd [33] Interface[256].Mtu changed from '1500' to '1490' by user 'admin' @ '192.168.10.77'

##### **TCP MSS option has been enabled:**

01/16/2004 08:52:26 0 tHttpd [33] Interface[256].TCPMSSEnabled changed from 'FALSE' to 'TRUE' by user 'admin' @ '192.168.10.77'

##### **TCP MSS option for LAN interface has been changed:**

01/16/2004 08:48:52 0 tHttpd [33] Interface[256].TCPMSSValue changed from '1360' to '1450' by user 'admin' @ '192.168.10.77'

##### **TCP MSS option has been disabled:**

01/16/2004 08:50:32 0 tHttpd [33] Interface[263].TCPMSSEnabled changed from 'TRUE' to '0' by user 'admin' @ '192.168.10.77'

##### **TCP MSS option has been re-enabled:**

01/16/2004 08:51:24 0 tHttpd [33] Interface[263].TCPMSSEnabled changed from 'FALSE' to '1' by user 'admin' @ '192.168.10.77'

##### **MTU for the branch office tunnel has been disabled:**

01/16/2004 08:53:36 0 tHttpd [33] DbGatewayGroups.Group[ou=Gateways, o=Bay Networks, c=US].Gateways.Gateway[cn=To CES1, ou=Gateways, o=Bay Networks, c=US].Accounts.Account[GENERAL,-].TunnelMTUEnabled changed from 'TRUE' to '0' by user 'admin' @ '192.168.10.77'

##### **MTU for the branch office has been enabled:**

01/16/2004 08:54:30 0 tHttpd [33] DbGatewayGroups.Group[ou=Gateways, o=Bay Networks, c=US].Gateways.Gateway[cn=To CES1, ou=Gateways, o=Bay Networks, c=US].Accounts.Account[GENERAL,-].TunnelMTUEnabled changed from 'FALSE' to '1' by user 'admin' @ '192.168.10.77'

##### **MTU for the tunnel has been changed from 1700 to 1701:**

01/16/2004 08:54:30 0 tHttpd [33] DbGatewayGroups.Group[ou=Gateways, o=Bay Networks, c=US].Gateways.Gateway[cn=To CES1, ou=Gateways, o=Bay Networks, c=US].Accounts.Account[GENERAL,-].TunnelMTU changed from '1700' to '1701' by user 'admin' @ '192.168.10.77'

##### **DF bit for the branch office group has been set:**

01/16/2004 08:56:39 0 tHttpd [33] DbGatewayGroups.Group[ou=Gateways, o=Bay Networks, c=US].Accounts.Account[IPSEC,-].IPSECDFBit changed from 'COPY' to 'SET' by user 'admin' @ '192.168.10.77'

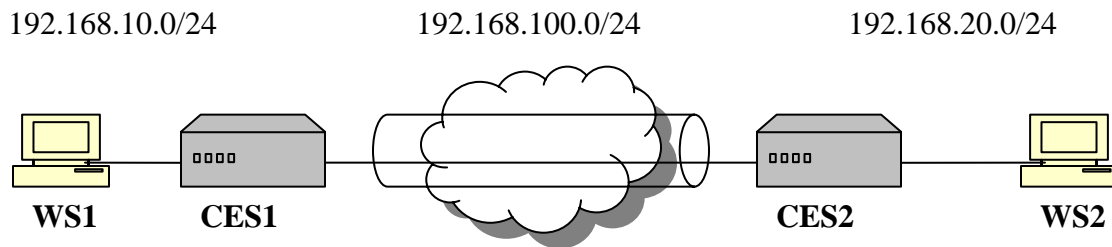
### Configurable MTU and TCP MSS clamping

---

## Sample Configurations

### Tunnel MTU

#### Setup



**WS1** – Windows 2000 workstation, IP 192.168.10.77/24;

**CES1** – Contivity Secure IP Services Gateway, management IP 192.168.10.1/24, private IP 192.168.10.10/24, public IP 192.168.100.1/24, code V04\_85;

**CES2** – Contivity Secure IP Services Gateway, management IP 192.168.20.2/24, private IP 192.168.20.20/24, public IP 192.168.100.2/24, code V04\_80;

**WS2** – Windows 2000 workstation, IP 192.168.20.55/24

The goal of the configuration is to configure an IPSec branch office tunnel between CES1 and CES2 and limit tunnel MTU on CES1 to 1200.

### Configuring WS1

Configure IP address on WS1 (192.168.10.77/24) with default gateway pointing to CES1 private interface (192.168.10.10):

```
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.10.77
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.10
```

# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

#### Configuring WS2

Configure IP address on WS2 (192.168.20.55/24) with default gateway pointing to CES2 private interface (192.168.20.20):

```
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.20.55
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.20.20
```

#### Configuring CES1

Configure IP address for management (192.168.10.1/24), private (192.168.10.10/24) and public (192.168.100.1/24) interfaces:

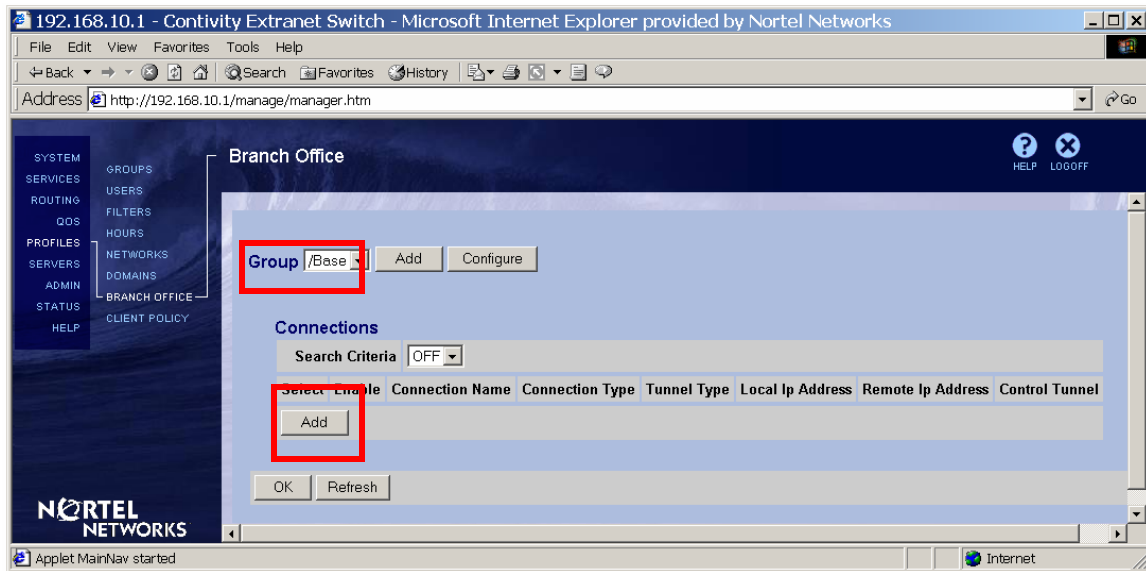
# Configuration Guide

## Contivity Secure IP Services Gateway

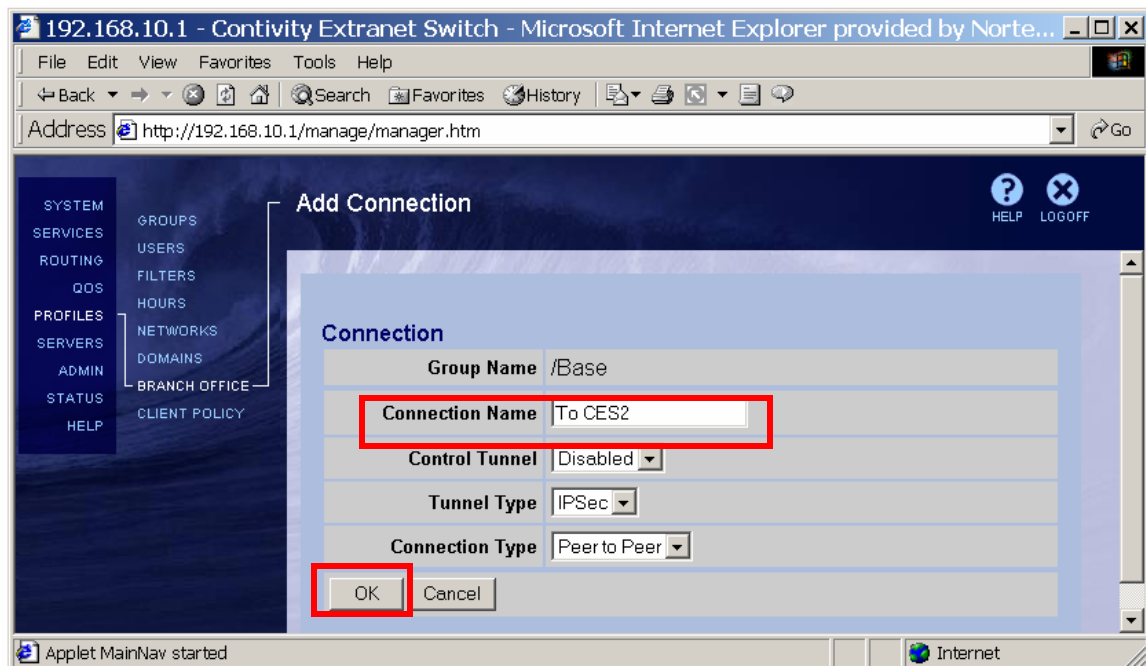


### Configurable MTU and TCP MSS clamping

Configure Branch Office. Navigate **Profiles**→**Branch Office**. Select a **Group** the tunnel will belong to (the default Base group will be used in this example). Click **Add** under the **Connections** section:



Enter the name for the connection (To CES2), leave the rest of the fields to their defaults and click **OK**:



# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

The **Connection Configuration** screen appears. Check the box next to **Enable** to enable BO connection:

Connection	
Group Name	/Base
Connection Name	To CES2
Control Tunnel	Disabled
Tunnel Type	IPSec
Connection Type	Peer to Peer
Enable	<input checked="" type="checkbox"/>

Select the **Local IP Address** (public IP address of CES1 – 192.168.100.1):

Endpoints	
Local Ip Address	(None)
Remote Ip Address	192.168.100.1

Enter the **Remote IP Address** (public IP address of CES2 – 192.168.100.2):

Endpoints	
Local Ip Address	192.168.100.1
Remote Ip Address	192.168.100.2

Leave the **Filter** to **permit all**:

Filters	
Filter	permit all

Leave the **Authentication** to **Text Pre-Shared Key**:

Authentication	
Text Pre-Shared Key	Text Pre-Shared Key

Enter the **Text Pre-Shared Key** (test):

Authentication	
Text Pre-Shared Key	Text Pre-Shared Key
Text Pre-Shared Key	Confirm

Make sure **MTU** is **Enabled** and enter the **MTU Value** (1200):

MTU	
Tunnel MTU	Enable
MTU Value	1200



# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

No NAT will be used in the example, so leave the **(None)** selection for **NAT**:

The image shows a configuration interface for NAT. It features a label "NAT" followed by a dropdown menu. The dropdown menu is currently set to "(None)".

Static IP Configuration will be used for this example:

The image shows a configuration interface for IP Configuration. It features a label "IP Configuration" followed by a dropdown menu. The dropdown menu is currently set to "Static".

Click **Create Local Network** under **Local Networks** section to define local network:

The image shows a configuration interface for Local Networks. It features a label "Local Networks" followed by a dropdown menu set to "(None)" and a button labeled "Create Local Network".

Enter the name (Loc192.168.10.0) for the local network to be created and click **Create**:

The image is a screenshot of a web browser window displaying the management interface of a Contivity Extranet Switch. The browser's address bar shows the URL "http://192.168.10.1/manage/manager.htm". The interface has a dark blue header with "192.168.10.1 - Contivity Extranet Switch - Microsoft Internet Explorer provided by Nortel Networks". A left sidebar contains a navigation menu with options like SYSTEM, SERVICES, ROUTING, QOS, PROFILES, SERVERS, ADMIN, STATUS, and HELP. The main content area is titled "Networks" and includes a "Return to Connection Configuration" link. Below this, there is a section titled "Current Networks" which states "(No networks defined)". At the bottom of this section, there is a "Create" button and a text input field containing the text "Loc192.168.10.0".

# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

The **Networks→Edit** screen appears. Enter the **IP Address** of the subnet (192.168.10.0) and **Mask** associated with the address (255.255.255.0). Click **Add**:

The configured subnet is listed under the **Current Subnets for the Network**. Click **Close**:

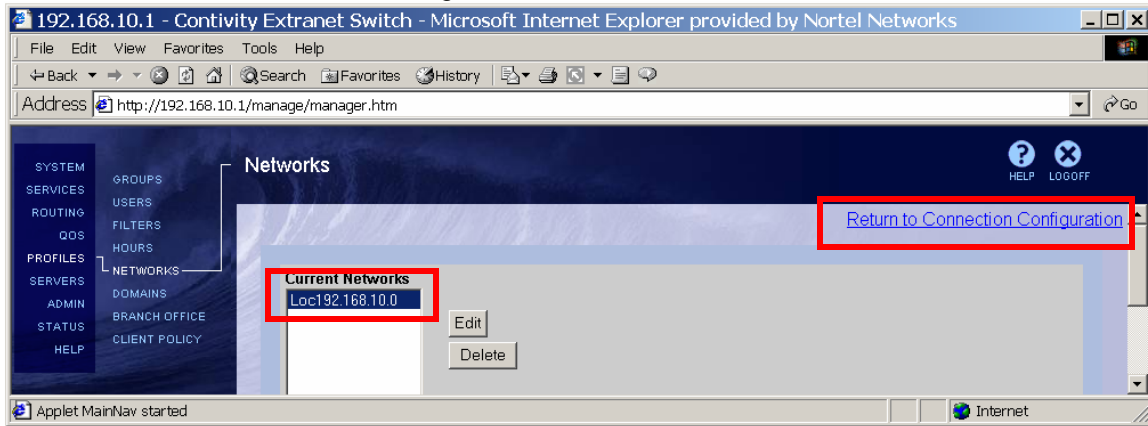
# Configuration Guide

## Contivity Secure IP Services Gateway

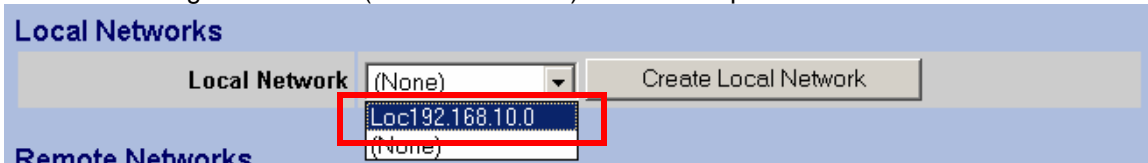


### Configurable MTU and TCP MSS clamping

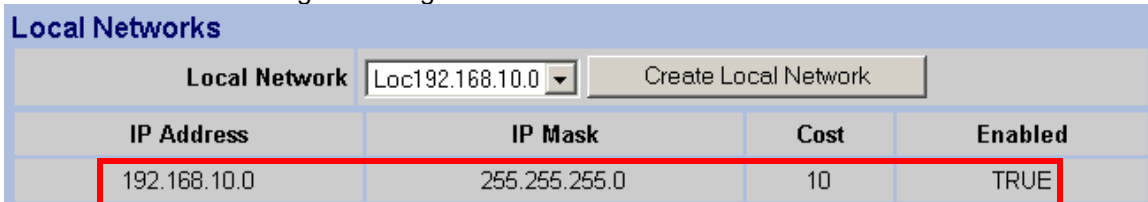
The configured network is listed under the **Current Networks**. Follow the link in the top right corner to return to branch office configuration:



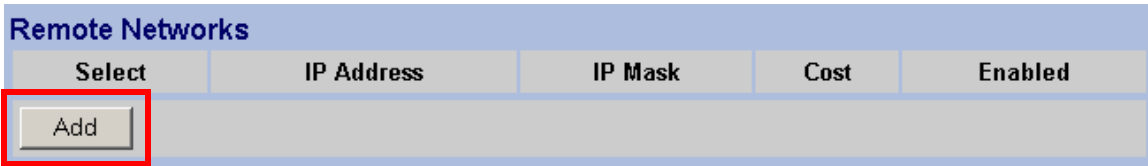
Select the configured network (Loc192.168.10.0) from the drop down list next to **Local Network**:



Screen refreshes showing the configured network:



Define remote reachable networks. Click **Add** under **Remote Networks**:



# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

The **Add Remote Network** screen appears. Enter the **IP Address** of remote network (CES2 private network – 192.168.20.0), **Mask** associated with the address (255.255.255.0), leave the **Cost** to default, make sure **Enabled** box is checked and click **OK**:

The configured network is listed under the **Remote Networks** section:

Remote Networks				
Select	IP Address	IP Mask	Cost	Enabled
<input checked="" type="radio"/>	192.168.20.0	255.255.255.0	10	<input checked="" type="checkbox"/>
<div>AddConfigureDelete</div>				

# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

Once all the parameters have been set, click **OK** at the bottom of the screen:

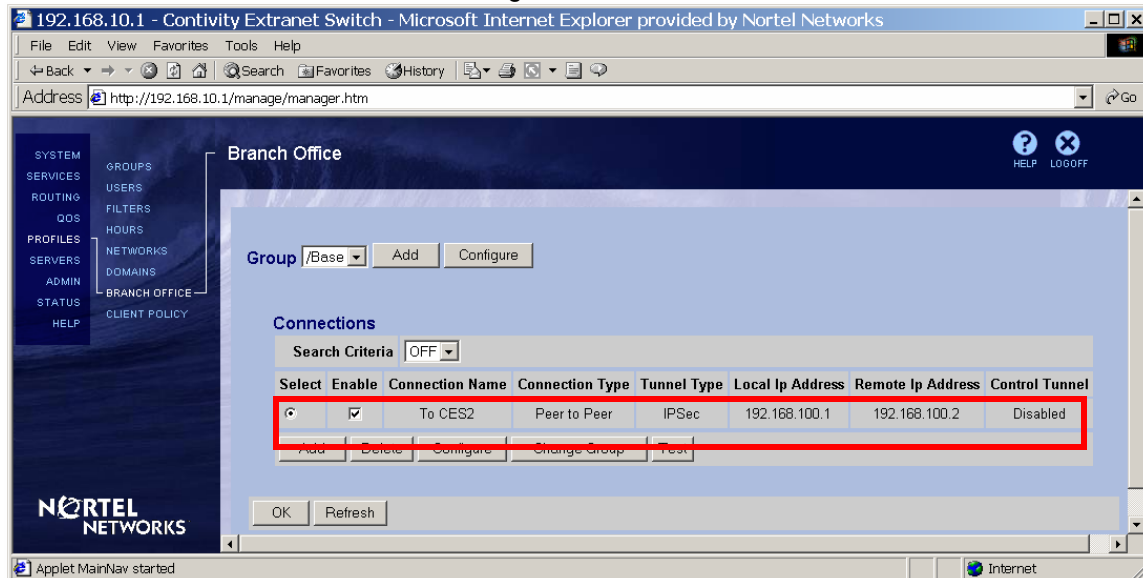
# Configuration Guide

## Contivity Secure IP Services Gateway



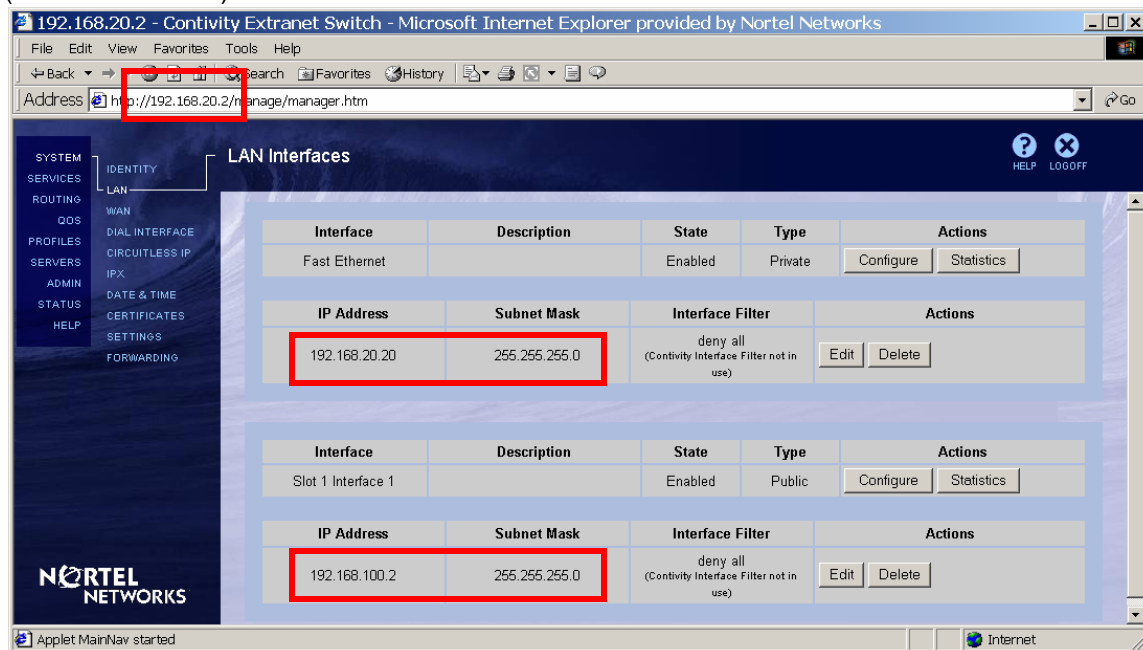
### Configurable MTU and TCP MSS clamping

BO connection from the CES1 side is configured:



### Configuring CES2

Configure IP address for management (192.168.20.2/24), private (192.168.20.20/24) and public (192.168.100.2/24) interfaces:



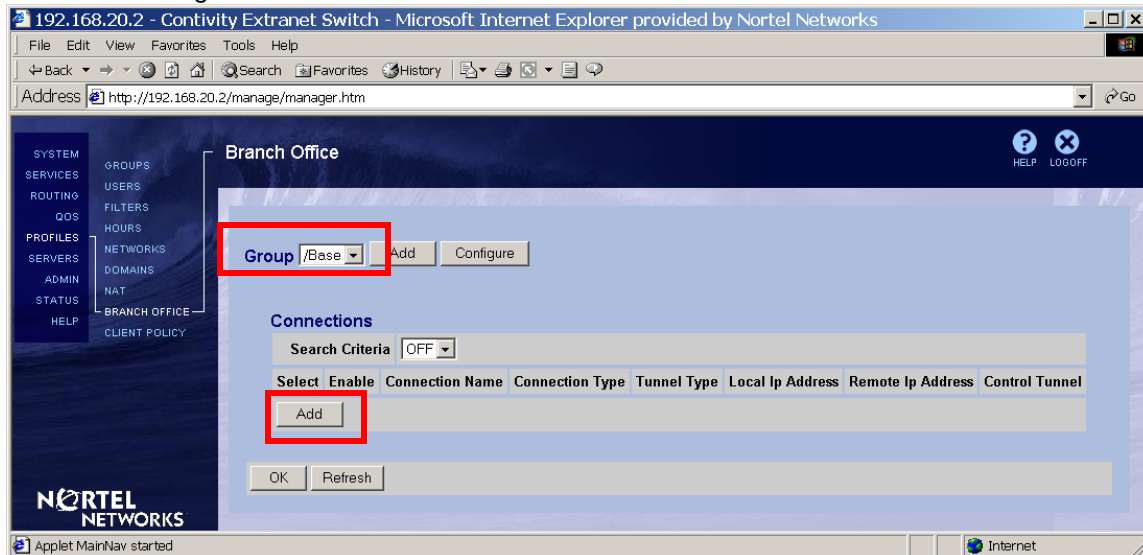
# Configuration Guide

## Contivity Secure IP Services Gateway

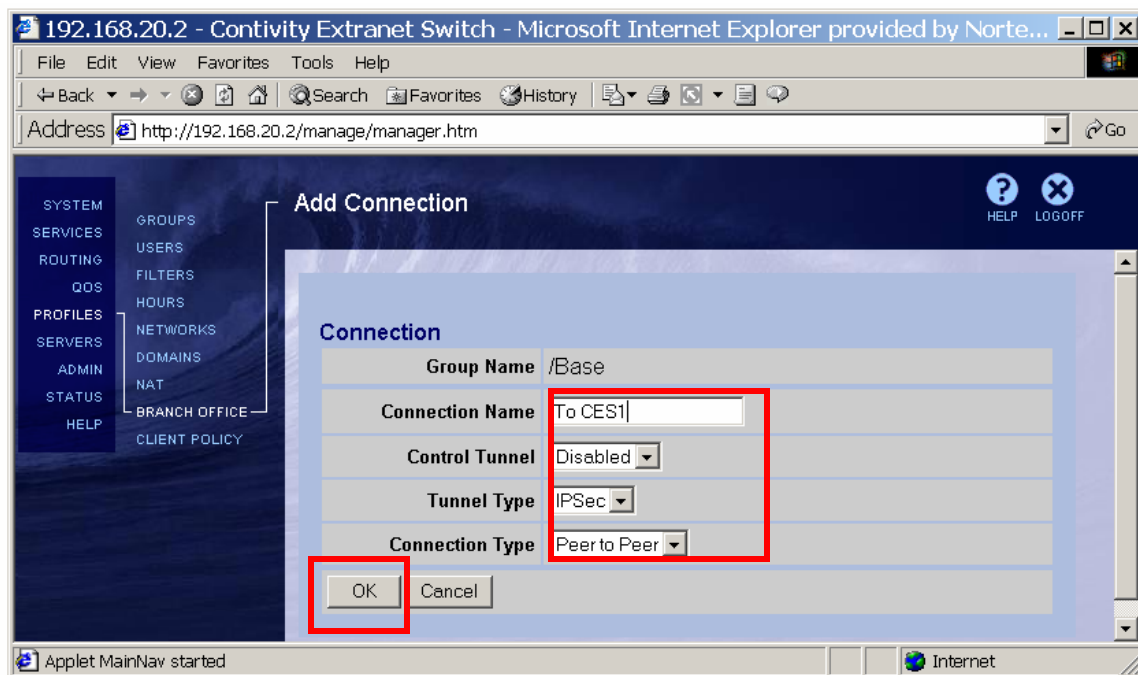


### Configurable MTU and TCP MSS clamping

Configure Branch Office connection. Navigate **Profiles**→**Branch Office**. Select a **Group** the tunnel will belong to and click **Add** under the **Connections**:



The **Add Connection** screen appears. Enter the name for the connection (To CES1), leave the rest of the fields to their defaults and click **OK**:



# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

The **Connection Configuration** screen appears. Check the box next to **Enable** to enable BO connection:

Connection	
Group Name	/Base
Connection Name	To CES2
Control Tunnel	Disabled
Tunnel Type	IPSec
Connection Type	Peer to Peer
Enable	<input checked="" type="checkbox"/>

Select the **Local IP Address** (public IP address of CES2 – 192.168.100.2):

Endpoints	
Local Ip Address	(None)
Remote Ip Address	192.168.100.2

Enter the **Remote IP Address** (public IP address of CES1 – 192.168.100.1):

Endpoints	
Local Ip Address	192.168.100.2
Remote Ip Address	192.168.100.1

Leave the **Filter** to **permit all**:

Filters	
Filter	permit all

Leave the **Authentication** to **Text Pre-Shared Key**:

Authentication	
Authentication	Text Pre-Shared Key

Enter the **Text Pre-Shared Key** (test):

Authentication	
Text Pre-Shared Key	Confirm

No NAT will be used in the example, so leave the **(None)** selection for **NAT**:

NAT	
NAT	(None)

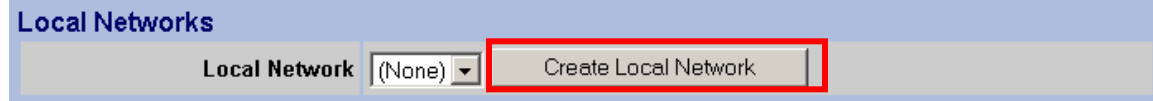
**Static IP Configuration** will be used for this example:

IP Configuration	
IP Configuration	Static

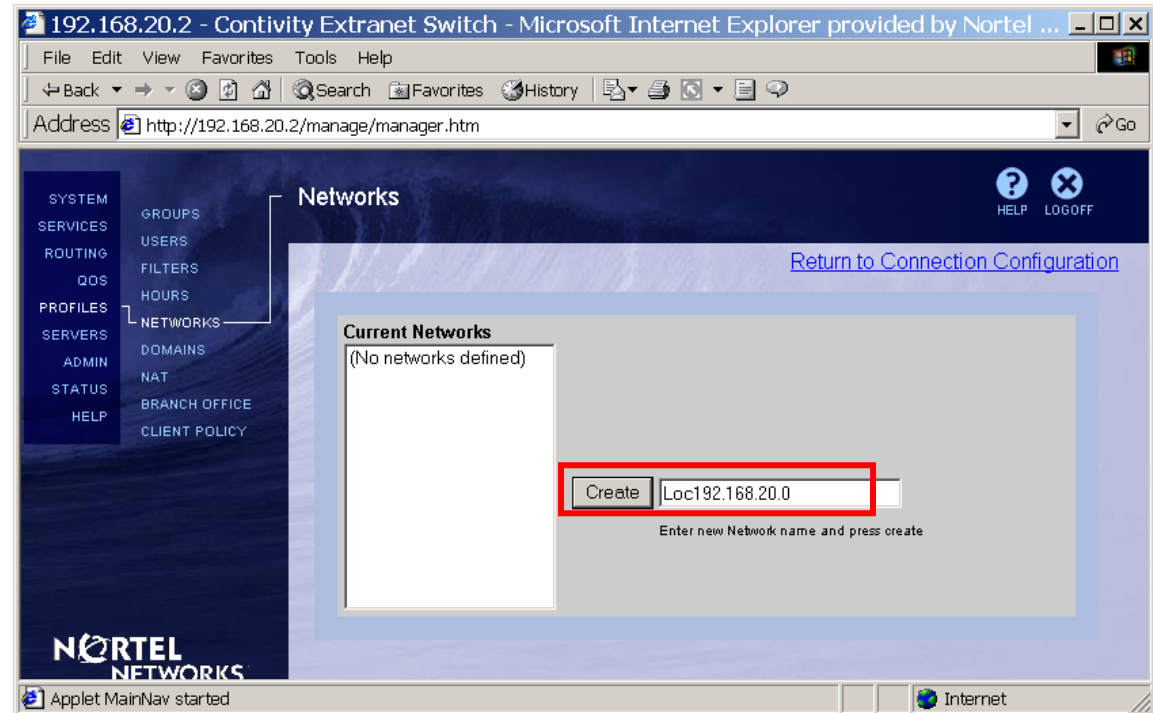


### Configurable MTU and TCP MSS clamping

Click **Create Local Network** under **Local Networks** section to define local network:



Enter the name (Loc192.168.20.0) for the local network to be created and click **Create**:



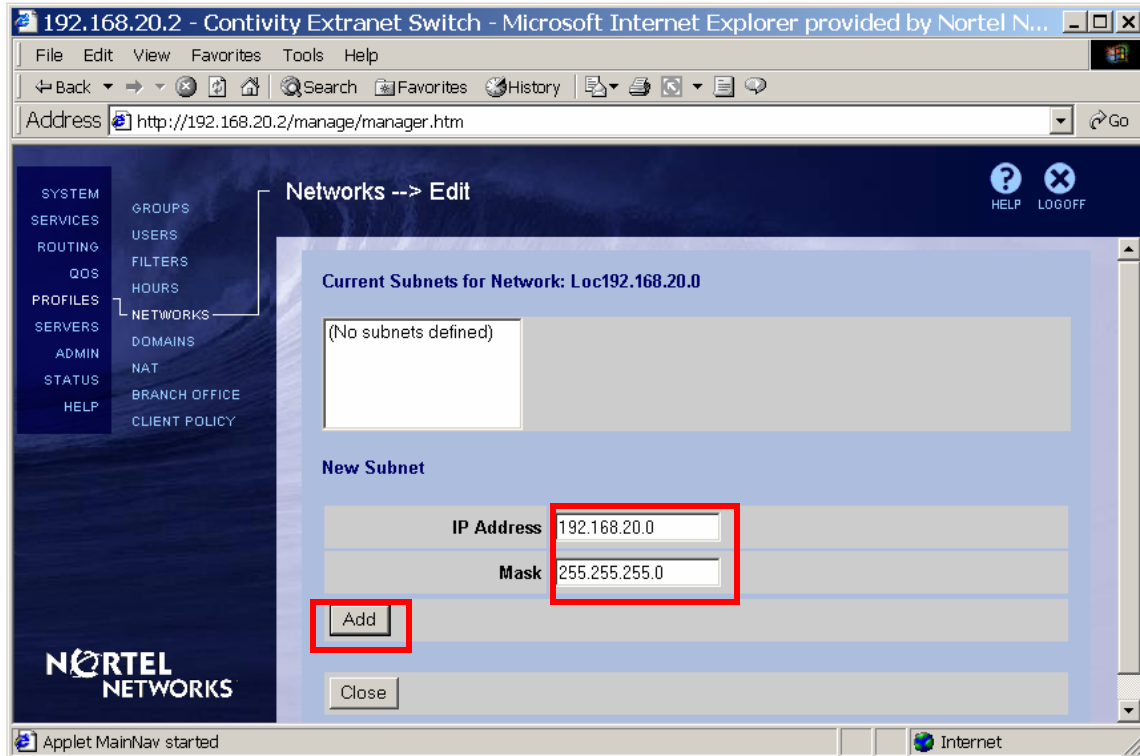
# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

The **Networks→Edit** screen appears. Enter the **IP Address** of the subnet (192.168.20.0) and **Mask** associated with the address (255.255.255.0). Click **Add**:



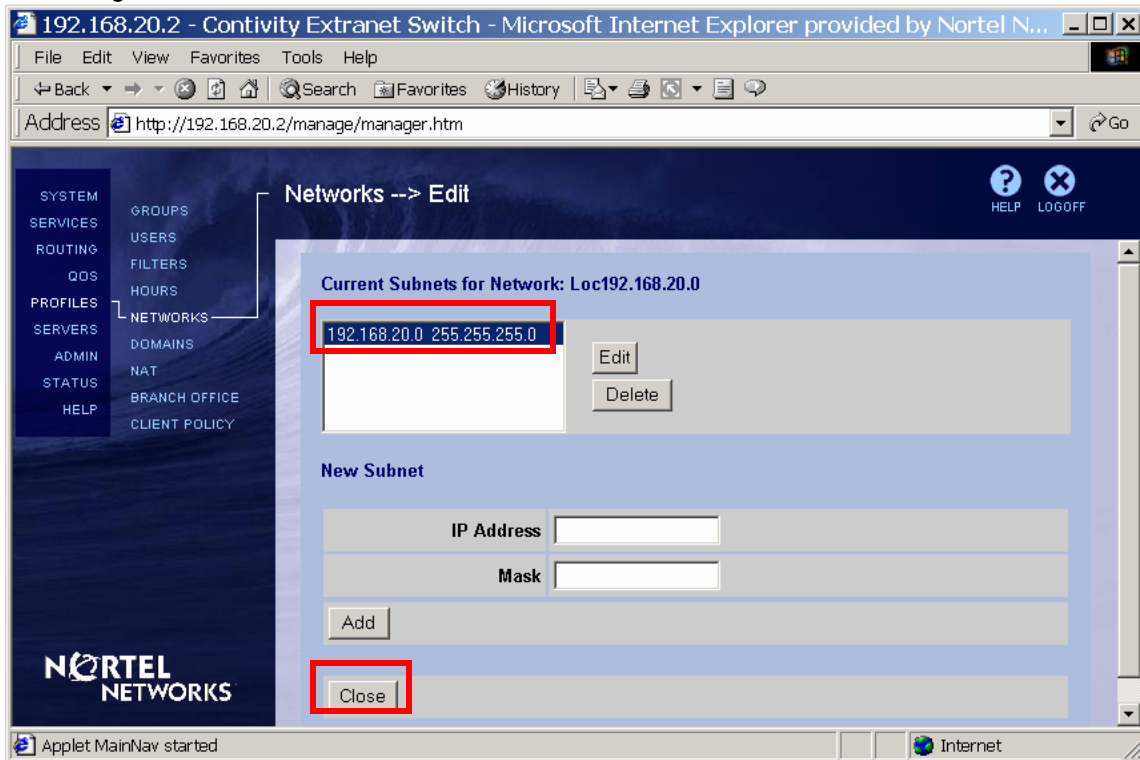
# Configuration Guide

## Contivity Secure IP Services Gateway

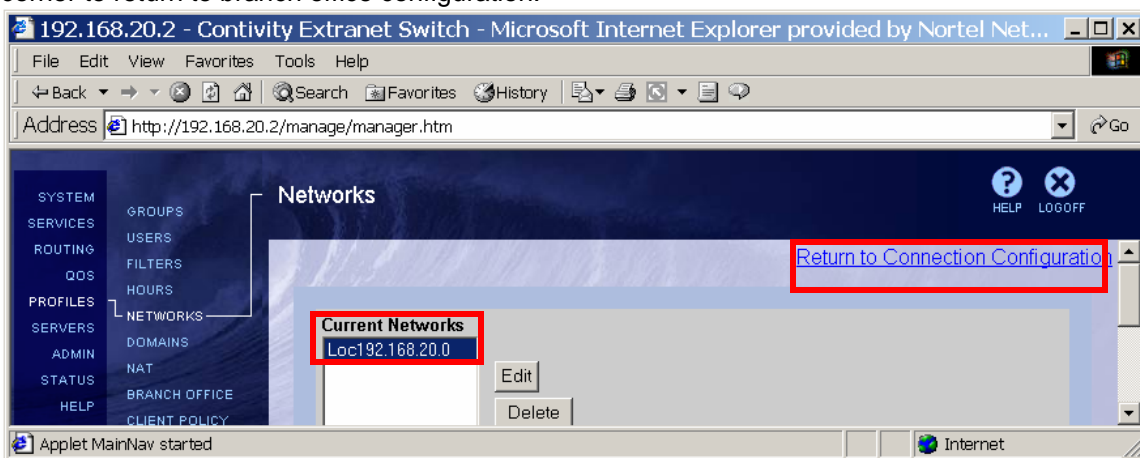


### Configurable MTU and TCP MSS clamping

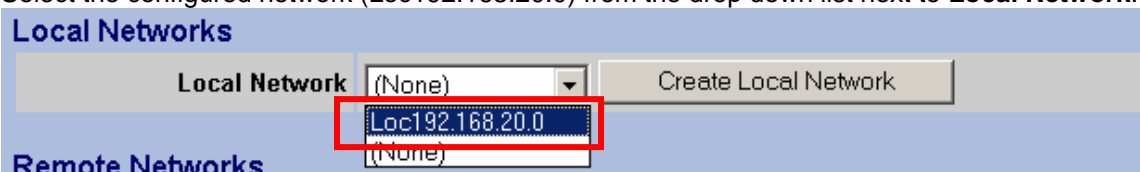
The configured subnet is listed under the **Current Subnets for the Network**. Click **Close**:



The configured network is listed under the **Current Networks**. Follow the link in the top right corner to return to branch office configuration:



Select the configured network (Loc192.168.20.0) from the drop down list next to **Local Network**:



### Configurable MTU and TCP MSS clamping

Screen refreshes showing the configured network:

**Local Networks**

Local Network: Loc192.168.20.0

IP Address	IP Mask	Cost	Enabled
192.168.20.0	255.255.255.0	10	TRUE

Define remote reachable networks. Click **Add** under **Remote Networks**:

**Remote Networks**

Select	IP Address	IP Mask	Cost	Enabled
<input type="button" value="Add"/>				

The **Add Remote Network** screen appears. Enter the **IP Address** of remote network (CES1 private network – 192.168.10.0), **Mask** associated with the address (255.255.255.0), leave the **Cost** to default, make sure **Enabled** box is checked and click **OK**:

192.168.20.2 - Contivity Extranet Switch - Microsoft Internet Explorer provided by Nortel ...

Address: http://192.168.20.2/manage/manager.htm

**Add Remote Network**

GROUPS  
USERS  
FILTERS  
HOURS  
NETWORKS  
DOMAINS  
NAT  
BRANCH OFFICE  
CLIENT POLICY

**Connection**

Group Name: /Base  
Connection Name: To CES1

**Remote Network**

IP Address: 192.168.10.0  
IP Mask: 255.255.255.0  
Cost: 10  
Enabled: ☒

NORTEL NETWORKS

Applet MainNav started

Internet

# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

The configured network is listed under the **Remote Networks** section:

**Remote Networks**

Select	IP Address	IP Mask	Cost	Enabled
<input checked="" type="radio"/>	192.168.10.0	255.255.255.0	10	<input checked="" type="checkbox"/>

Add Configure Delete

Once all the parameters have been set, click **OK** at the bottom of the screen:

192.168.20.2 - Contivity Extranet Switch - Microsoft Internet Explorer provided by Nortel Networks

Address http://192.168.20.2/manage/manager.htm

**Connection Configuration**

This page has been modified. Please click the OK/Apply button to send configuration changes to the device. Or, please click the Refresh button to get the latest data from the device and clear all changes.

**Connection**

Group Name /Base

Connection Name To CES1

Control Tunnel Disabled

Tunnel Type IPSec

Connection Type Peer to Peer

Enable ☒

**Endpoints**

Local Ip Address 192.168.100.2

Remote Ip Address 192.168.100.1

**Filters**

Filter permit all

**Authentication** Text Pre-Shared Key

Text Pre-Shared Key Confirm

**NAT**

NAT (None)

**IP Configuration** Static

**Local Networks**

Local Network Loc192.168.20.0 Create Local Network

IP Address	IP Mask	Cost	Enabled
192.168.20.0	255.255.255.0	10	TRUE

**Remote Networks**

Select	IP Address	IP Mask	Cost	Enabled
<input checked="" type="radio"/>	192.168.10.0	255.255.255.0	10	<input checked="" type="checkbox"/>

Add Configure Delete

OK Cancel Apply Refresh

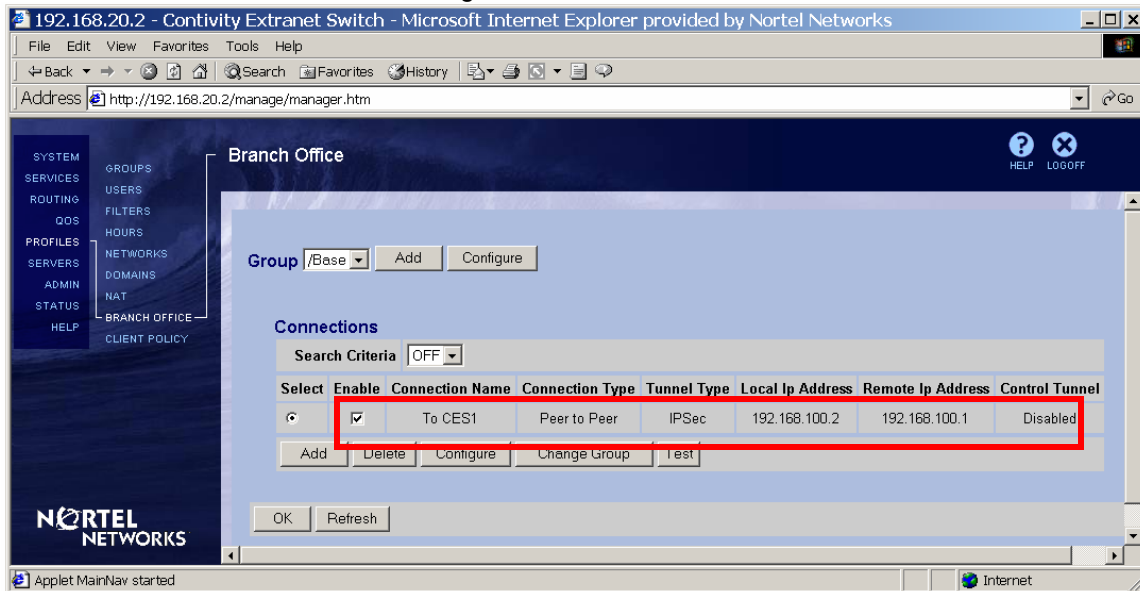
# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

BO connection from CES2 side is configured:



### Testing configuration

Ping from WS1 (192.168.10.77) to WS2 (192.168.20.55) to bring the BO connection up:

```
C:\>ping 192.168.20.55
Pinging 192.168.20.55 with 32 bytes of data:
Reply from 192.168.20.2: TTL expired in transit.
Reply from 192.168.20.55: bytes=32 time<10ms TTL=28
Reply from 192.168.20.55: bytes=32 time<10ms TTL=28
Reply from 192.168.20.55: bytes=32 time<10ms TTL=28

Ping statistics for 192.168.20.55:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

BO connection is established and ping goes through.

Set up a sniffer to capture packets on interface between CES2 and WS2. Ethereal software was used in this example on WS2 to capture packets.

# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

Ping from WS1 to WS2 and send a packet larger than configured tunnel MTU. As we configured tunnel MTU to be 1200, let's send a ping with a data size of 1400:

```
C:\>ping 192.168.20.55 -l 1400
Pinging 192.168.20.55 with 1400 bytes of data:
Reply from 192.168.20.55: bytes=1400 time=10ms TTL=28
Reply from 192.168.20.55: bytes=1400 time=10ms TTL=28
Reply from 192.168.20.55: bytes=1400 time=10ms TTL=28
Reply from 192.168.20.55: bytes=1400 time=10ms TTL=28
Ping statistics for 192.168.20.55:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 10ms, Average = 10ms
```

Stop the capture. Take a look at the ICMP packets sent/received. As we configured tunnel MTU on CES1 to be 1200, CES1 fragments ICMP packets to fit the configured MTU and WS2 receives fragmented ICMP packets. CES2 used a default value for MTU (1788) and therefore ICMP packets traveling back to WS1 will not be fragmented:

The screenshot shows a Wireshark capture titled 'PRIVATE20.cap - Ethereal'. The packet list shows 12 packets. Packets 1, 3, 5, 7, 9, 11 are ICMP Echo (ping) requests from 192.168.10.77 to 192.168.20.55. Packets 2, 4, 6, 8, 10, 12 are fragmented IP protocols (proto=ICMP 0x01, off=1120) from 192.168.10.77 to 192.168.20.55. Packets 1, 3, 5, 7, 9, 11 are ICMP Echo (ping) replies from 192.168.20.55 to 192.168.10.77. Packets 2, 4, 6, 8, 10, 12 are fragmented IP protocols (proto=ICMP 0x01, off=1120) from 192.168.20.55 to 192.168.10.77.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.10.77	192.168.20.55	ICMP	Echo (ping) request
2	0.000000	192.168.10.77	192.168.20.55	IP	Fragmented IP protocol (proto=ICMP 0x01, off=1120)
3	0.000000	192.168.10.77	192.168.20.55	ICMP	Echo (ping) request
4	1.000000	192.168.10.77	192.168.20.55	IP	Fragmented IP protocol (proto=ICMP 0x01, off=1120)
5	1.000000	192.168.10.77	192.168.20.55	ICMP	Echo (ping) request
6	1.000000	192.168.10.77	192.168.20.55	IP	Fragmented IP protocol (proto=ICMP 0x01, off=1120)
7	2.000000	192.168.10.77	192.168.20.55	ICMP	Echo (ping) request
8	2.000000	192.168.10.77	192.168.20.55	IP	Fragmented IP protocol (proto=ICMP 0x01, off=1120)
9	2.000000	192.168.10.77	192.168.20.55	ICMP	Echo (ping) request
10	3.000000	192.168.10.77	192.168.20.55	IP	Fragmented IP protocol (proto=ICMP 0x01, off=1120)
11	3.000000	192.168.10.77	192.168.20.55	ICMP	Echo (ping) request
12	3.000000	192.168.10.77	192.168.20.55	IP	Fragmented IP protocol (proto=ICMP 0x01, off=1120)

A close look at packets from the tunnel shows that CES1 fragmented ICMP packet with 1400 bytes of data into one packet with 1112 bytes of data and one with 288 bytes of data:

The screenshot shows the packet details for two packets. Packet 1 is an ICMP Echo (ping) request from 192.168.10.77 to 192.168.20.55. The data field is highlighted with a red box and labeled 'Data (1112 bytes)'. Packet 2 is an IP Fragmented IP protocol (proto=ICMP 0x01, off=1120) from 192.168.10.77 to 192.168.20.55. The data field is highlighted with a red box and labeled 'Data (288 bytes)'. The packet bytes are shown at the bottom.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.10.77	192.168.20.55	ICMP	Echo (ping) request
2	0.000000	192.168.10.77	192.168.20.55	IP	Fragmented IP protocol (proto=ICMP 0x01, off=1120)



# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

Start capture on WS1. Send a ping from WS1 to WS2 with a large data (1400) and DF bit set. Note the returned by CES1 ICMP message - packet needs to be fragmented but DF bit set:

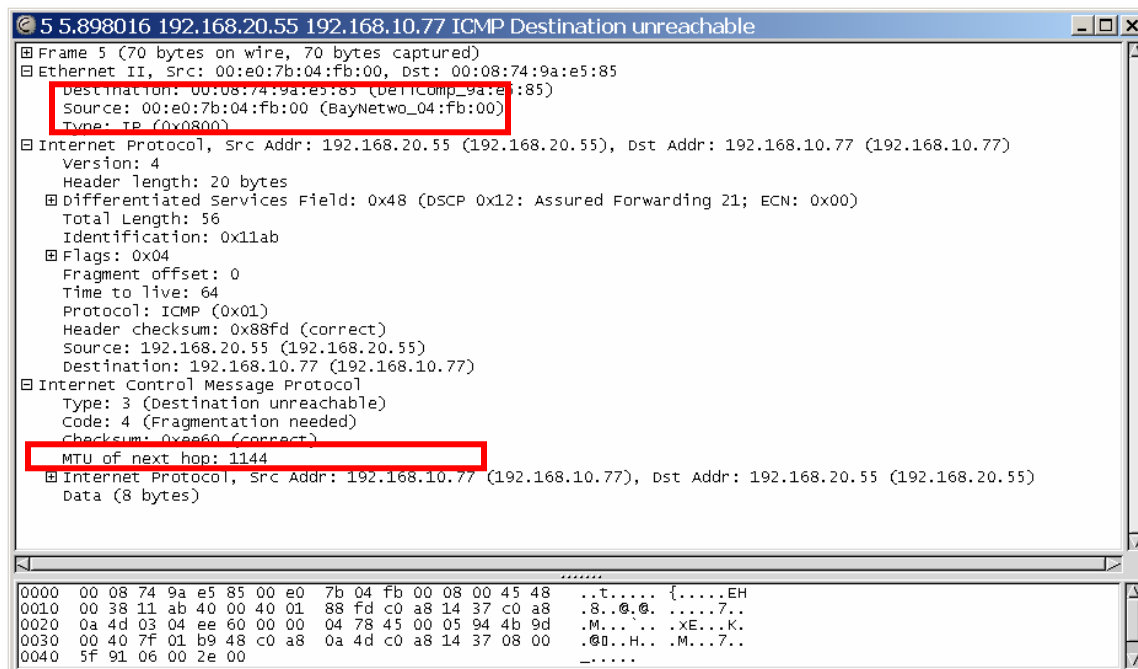
```
C:\>ping 192.168.20.55 -l 1400 -f
Pinging 192.168.20.55 with 1400 bytes of data:
Reply from 192.168.20.55: Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 192.168.20.55:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If you take a look at the ARP table on WS and compare the MAC address associated with 192.168.10.10 (CES1 private interface) with the source address of the received ICMP message in the captured trace, you'll see that ICMP was sent by CES1:

```
C:\>arp -a
Interface: 192.168.10.77 on Interface 0x1000007
Internet Address      Physical Address      Type
192.168.10.10         00-e0-7b-04-fb-00     dynamic
```

Note also that CES1 supplies the correct MTU to be used in the MTU of next hop field of the ICMP message:



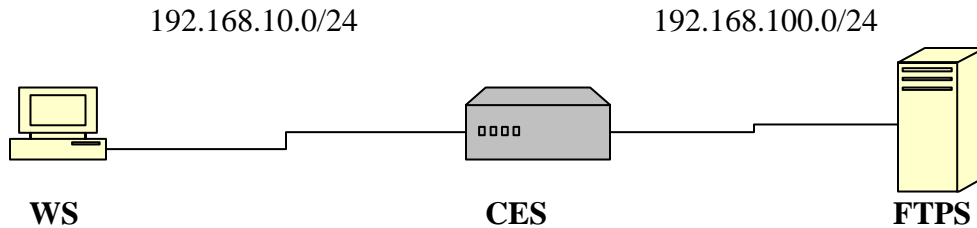


### Configurable MTU and TCP MSS clamping

---

## TCP MSS Clamping

### Setup



**WS** – Windows 2000 workstation, IP 192.168.10.77/24;

**CES** – Contivity Secure IP Services Gateway, management IP 192.168.10.1/24, private IP 192.168.10.10/24, public IP 192.168.100.1/24;

**FTPS** – Nortel Networks ANH 8 port router-hub with FTP service enabled, IP 192.168.100.3/24

The goal of the configuration is to configure CES to use TCP MSS option to limit the packet size.

### Configuring WS

Configure IP address on WS1 (192.168.10.77/24) with default gateway pointing to CES1 private interface (192.168.10.10):

```
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.10.77
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.10
```

# Configuration Guide

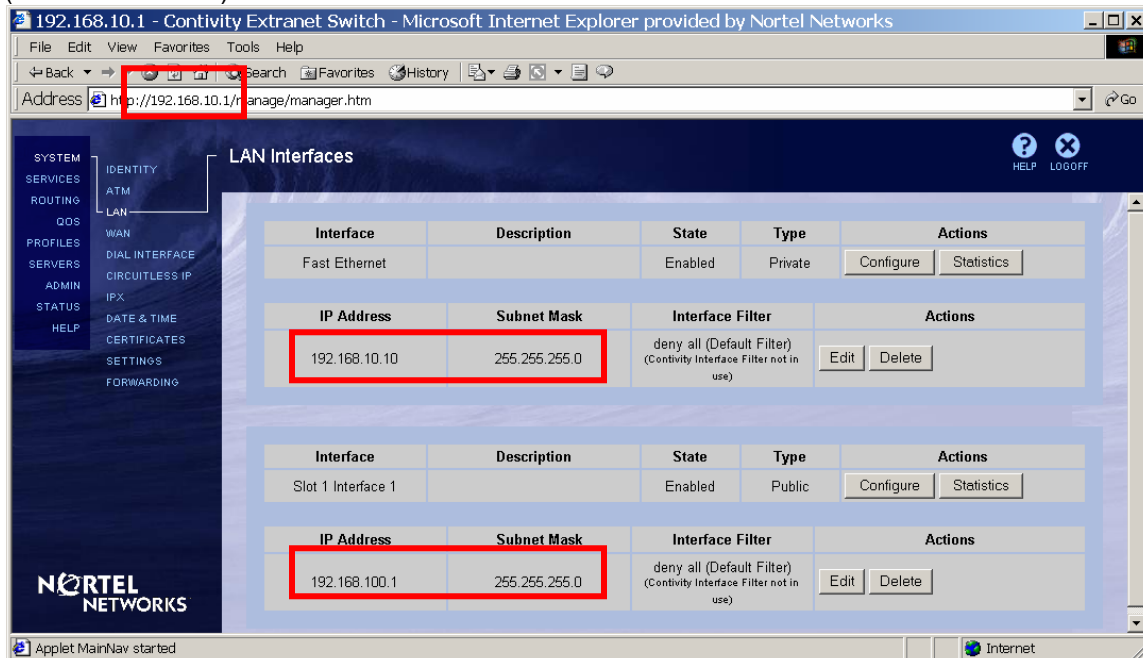
## Contivity Secure IP Services Gateway



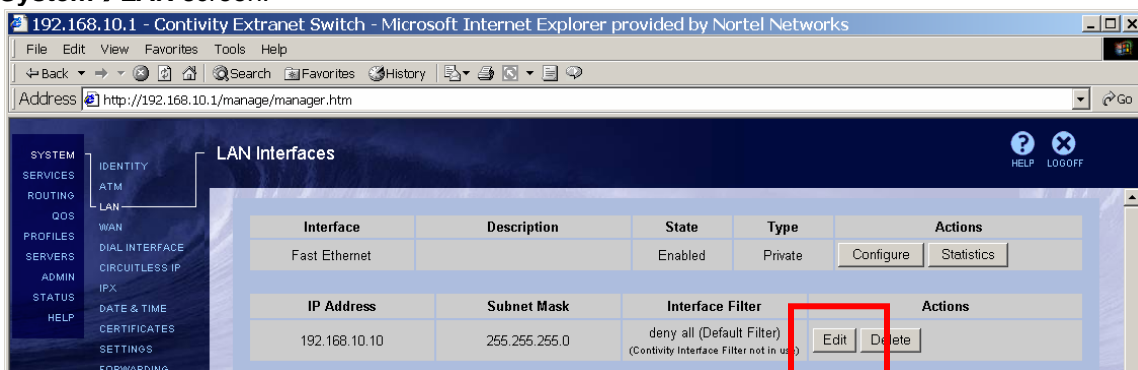
### Configurable MTU and TCP MSS clamping

#### Configuring CES

Configure IP address for management (192.168.10.1/24), private (192.168.10.10/24) and public (192.168.100.1/24) interfaces:



Allow traffic from WS to FTPS. The goal of the configuration is to show the work of TCP MSS option only, so permit all filter will be used in this example for simplicity. Apply permit all interface filter to private interface (192.168.10.10) on the **System→LAN** screen:



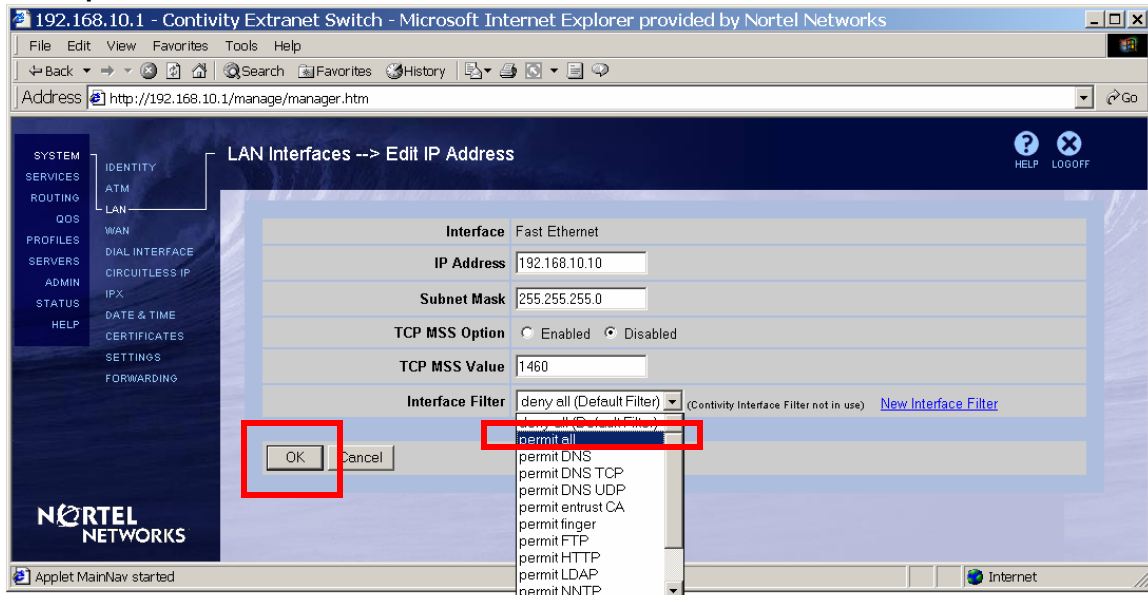
# Configuration Guide

## Contivity Secure IP Services Gateway

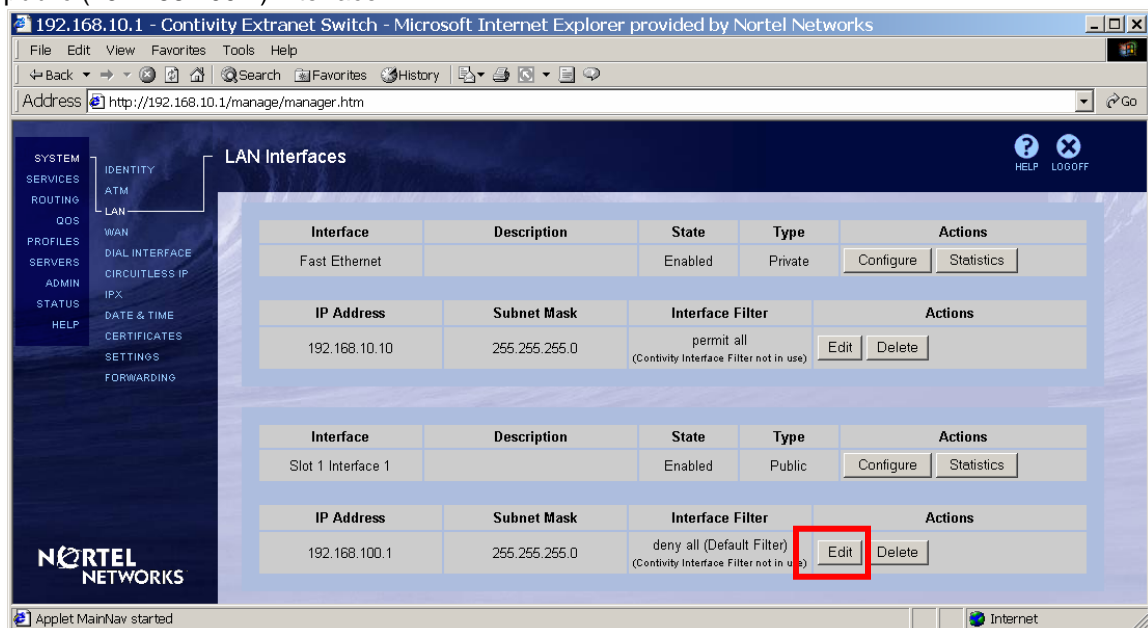


### Configurable MTU and TCP MSS clamping

Select **permit all** interface filter and click **OK**:



Apply permit all filter to the public interface and configure TCP MSS option. Click **Edit** next to public (192.168.100.1) interface:



# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

Select **Enable** for the **TCP MSS Option**. Enter the **Value** for the MSS (540 in this example), select **permit all** interface filter and click **OK**:

# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

Enable Interface Filters globally on Contivity. Navigate **Services→Firewall/NAT**. Check the box next to **Contivity Interface Filter** and click **OK** at the bottom of the page:

192.168.10.1 - Contivity Extranet Switch - Microsoft Internet Explorer provided by Nortel Networks

Address: http://192.168.10.1/manage/manager.htm

**Firewall / NAT**

**Configuration**

Enabled	Firewall / NAT Type	Firewall / NAT Policy	Action
<input checked="" type="checkbox"/>	Contivity Firewall *		<a href="#">Edit</a>
	Contivity Stateful Firewall Not available until a license key is installed.		
<input checked="" type="checkbox"/>	Contivity Interface Filter		
<input type="checkbox"/>	Interface NAT	NAT Policy: (None)	<a href="#">Manage Policies</a>
<input type="checkbox"/>	Anti-Spoofing		<a href="#">Edit</a>
<input type="checkbox"/>	Malicious Scan Detection		<a href="#">Edit</a>
<input type="checkbox"/>	No Firewall		

\* A Firewall must be enabled to allow interface traffic, select either interface(packet) filters, or the Contivity Stateful Firewall

**Contivity Tunnel Filter** ☒ Enable

**Contivity Tunnel Management Filter** ☒ Enable

\* Contivity Tunnel Filter and Contivity Tunnel Management Filter can only be disabled when Contivity Stateful Firewall is enabled. It is typically enabled while you are migrating to the Stateful Firewall.

\* Disabling Tunnel Management Filters requires that specific rules to be created in the Contivity Stateful Firewall enabling inbound management service traffic (such as HTTP and PING) through tunnel. A stateful firewall rule formatted in this manner will accomplish this:

Src Interface	Dst Interface	Source	Destination	Service	Action
Tunnel:Any	System	Any	Any	Contivity-Management	Allow

**TunnelGuard Configuration**

Server Port: 8282

**Rule Configuration**

[Manage Policies](#)

\* Note : The rule configuration Java applet is digitally signed by Contivity. To verify the certificate signature authenticity you can contact Nortel Product Support.

[OK](#) [Cancel](#) [Refresh](#)

Enabling Interface filters requires Contivity to be rebooted. Follow the **Schedule System Reboot** link on the top of the screen and complete a reboot:

The following changes to Firewall/NAT settings will not take effect until you reboot the system :  
Switching to Contivity Interface Filter (Currently running No Firewall)  
[Schedule System Reboot](#)

### Configurable MTU and TCP MSS clamping

---

#### Configuring FTPS

BCC or Site Manager can be used to configure the ANH; BCC is used in this example. Log in to the router and enter the bcc configuration mode:

```
Login: Manager
      Welcome to the Backbone Technician Interface

[1:1]$ bcc
      Welcome to the Bay Command Console!
      * To enter configuration mode, type config
      * To list all system commands, type ?
      * To exit the BCC, type exit
bcc>
```

Enter the configuration mode:

```
bcc> config
Reading configuration information, please wait . . . done.
box#
```

Configure the IP address (192.168.50.7/24) for the Ethernet interface:

```
box# eth 1/1;ip 192.168.100.3/24;state enabled
ip/192.168.100.3/255.255.255.0#
```

Enable FTP service:

```
ip/192.168.100.3/255.255.255.0#box;ftp
ftp#
```

Configure FTPS to use CES1 public IP as a default gateway:

```
ftp# ip; static-route 0.0.0.0/0.0.0.0/192.168.100.1
static-route/0.0.0.0/0.0.0.0/192.168.100.1#
```

### Configurable MTU and TCP MSS clamping

---

#### Testing configuration

Make sure you can ping FTPS (192.168.100.3) from WS (192.168.10.77):

```
C:\>ping 192.168.100.3
Pinging 192.168.100.3 with 32 bytes of data:
Reply from 192.168.100.3: bytes=32 time=101ms TTL=29
Reply from 192.168.100.3: bytes=32 time<10ms TTL=29
Reply from 192.168.100.3: bytes=32 time<10ms TTL=29
Reply from 192.168.100.3: bytes=32 time<10ms TTL=29

Ping statistics for 192.168.100.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 101ms, Average = 25ms
```

Set up two sniffers one on the private side of CES and one on the public side of CES. Contivity PCAP will be used in this example to capture packets on public interface. For information on PCAP please consult *Configuration Guide - PCAP on Contivity*. Ethereal software will be used to capture traffic on private side.

Make sure the password for the administrator is changed from default “setup”. To change password to for example “test” via CLI, login in to CES, enter the privileged mode and enter the configuration mode:

```
CES#conf t
Enter configuration commands, one per line.  End with Ctrl/z.
CES(config)#adminname admin password test
```

Enable capture, select a password to protect the capture (1qazxsw2 is used in this example):

```
CES#cap ena
Please specify password for encrypting capture files.
Password: *****
Reenter password: *****
```

Configure a capture to be taken on public interface (FastEthernet in this example) with default settings and named tcp-pub:

```
CES#cap add tcp-pub fast 1/1
```

Start the capture:

```
CES#cap tcp-pub start
```

Start the capture in Ethereal on WS. Note: PCAP can also be used to capture packets on private side. We used Ethereal on private side as an example only.

# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

---

Open an FTP session to FTPS, enter User ID (Manager is the default User ID for ANH):

```
C:\>ftp 192.168.100.3
Connected to 192.168.100.3.
220 WfFTP server(x13.20) ready.
User (192.168.100.3:(none)): Manager
230 User Manager logged in.
```

Issue a dir command to view the contents of the directory:

```
ftp> dir
200 PORT command successful.
150 ASCII data connection for 1: (192.168.100.3,20) (0 bytes).

Volume - drive 1:
Directory of 1:

File Name                               Size      Date      Day      Time
-----
startup.cfg                             2116    03/06/03   Thur.    07:38:50
configPppChap                           2996    03/12/03   Wed.     16:43:58
bgpOspf.log                             32428   03/20/03   Thur.    13:08:26
an.exe                                  7112672  03/20/03   Thur.    13:18:09
bcc.help                                492551   03/20/03   Thur.    13:21:43
debug.al                                 12319   03/20/03   Thur.    13:22:46
install.bat                             236499   03/20/03   Thur.    13:22:54
ti.cfg                                  132     03/20/03   Thur.    13:23:09
log2.log                                32428   03/20/03   Thur.    14:31:46
configFrRip                             386     07/18/03   Fri.     12:02:25
config                                  1720    07/25/03   Fri.     08:52:00
hosts                                    17      09/04/03   Thur.    15:56:51

33554432 bytes - Total size
25627726 bytes - Available free space
17672120 bytes - Contiguous free space
226 ASCII Transfer Complete.
ftp: 938 bytes received in 0.00Seconds 938000.00Kbytes/sec.
```

Get some file large file from the FTPS, file named bcc.help was downloaded in this example:

```
ftp> get bcc.help
200 PORT command successful.
150 Image data connection for 1:bcc.help (192.168.100.3,0) (492551
bytes).
226 Binary Transfer Complete.
ftp: 492551 bytes received in 9.71Seconds 45.54Kbytes/sec.
```



### Configurable MTU and TCP MSS clamping

---

Close the FTP session:

```
ftp> quit
221 Goodbye.
```

Stop and save capture:

```
CES#cap tcp-pub stop
CES#cap tcp-pub save tcp
Saving capture tcp to file /ide0/tcp-pub please wait . . .
176 frames written successfully
```

Stop the capture in Ethereal.

Enable ftp on CES:

```
CES#conf t
Enter configuration commands, one per line.  End with Ctrl/z.
CES(config)#ftp-server enable
CES(config)#exit
CES#
```

FTP saved capture file to WS, make sure to use binary mode:

```
C:\>ftp 192.168.10.1
Connected to 192.168.100.3.
220 WfFTP server(x13.20) ready.
User (192.168.100.3:(none)): admin
331 Password required for admin.
Password:
230 User Manager logged in.
ftp> bin
200 Type set to I.
ftp> get tcp-pub
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
ftp: 47972 bytes received in 0.17Seconds 282.19Kbytes/sec.
ftp> quit
221 Bye...see you later
```

Decrypt capture file with openpcap.exe:

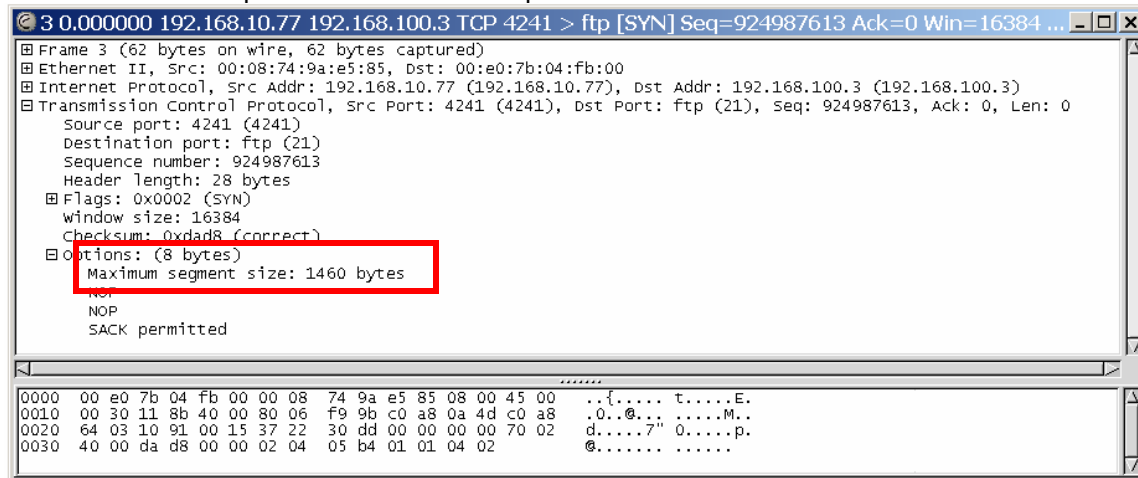
```
D:\tmp\openpcap>openpcap.exe tcp-pub tcp-pub.cap
Password:
```

### Configurable MTU and TCP MSS clamping

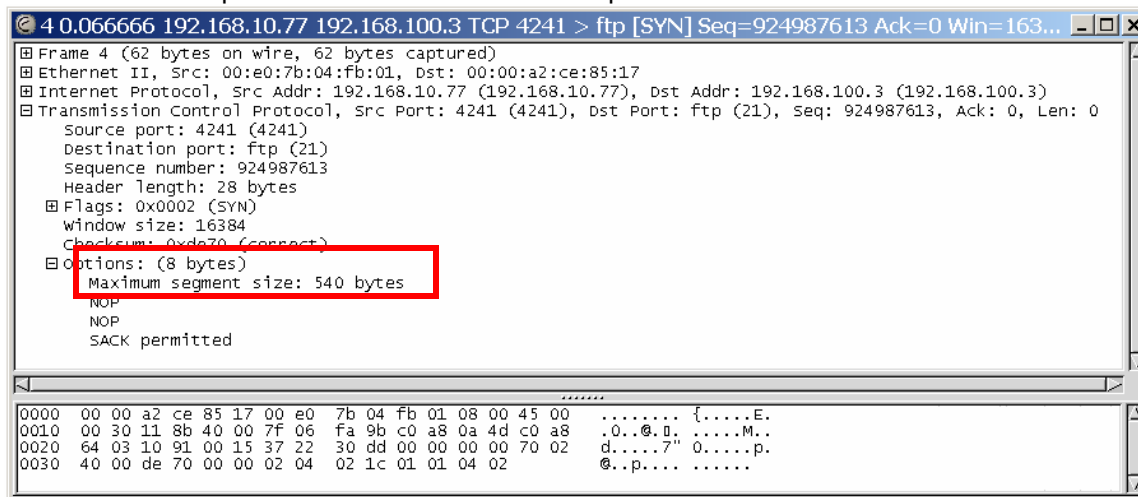
Open the decrypted capture with Ethereal. Compare TCP traffic before and after it reaches CES.

Note the following:

WS sends first TCP packet with TCP MSS option set to 1460:



CES transfers the packet to FTPS with TCP MSS option set to 540:



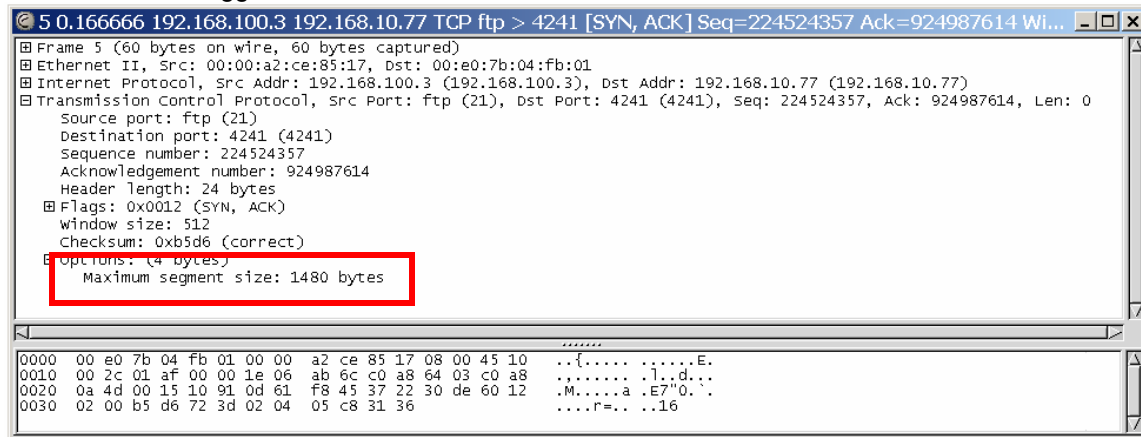
# Configuration Guide

## Contivity Secure IP Services Gateway

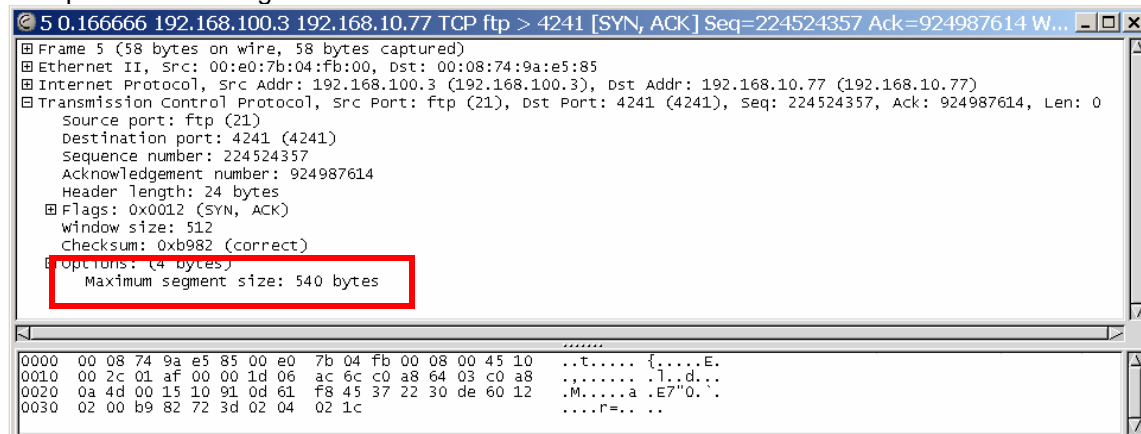


### Configurable MTU and TCP MSS clamping

FTPS sends its suggestion to use 1480 TCP MSS:



CES passes this along to WS with TCP MSS set to 540:



This way both WS and FTPS learn not to send each other packets with TCP data larger than TCP MSS, 540 bytes.

# Configuration Guide

## Contivity Secure IP Services Gateway



### Configurable MTU and TCP MSS clamping

So when a transfer begins, packets will be limited in size according to the TCP MSS settings:

No.	Time	Source	Destination	Protocol	Info
37	19.733333	192.168.100.3	192.168.10.77	FTP	Response: 150 image data connection for 1:bcc.help (192.168.100.3)
38	19.800000	192.168.100.3	192.168.10.77	FTP-DATA	FTP Data: 508 bytes
39	19.800000	192.168.100.3	192.168.10.77	FTP-DATA	FTP Data: 508 bytes
40	19.800000	192.168.100.3	192.168.10.77	FTP-DATA	FTP Data: 66 bytes
41	19.800000	192.168.10.77	192.168.100.3	TCP	4243 > ftp-data [ACK] Seq=930030791 Ack=224530382 win=16740 Len=0
42	19.883333	192.168.10.77	192.168.100.3	TCP	4243 > ftp-data [ACK] Seq=930030791 Ack=2245324656 win=16442 Len=0
43	19.950000	192.168.100.3	192.168.10.77	FTP-DATA	FTP Data: 502 bytes
44	19.950000	192.168.100.3	192.168.10.77	FTP-DATA	FTP Data: 508 bytes
45	19.950000	192.168.100.3	192.168.10.77	FTP-DATA	FTP Data: 508 bytes
46	19.950000	192.168.10.77	192.168.100.3	TCP	4243 > ftp-data [ACK] Seq=930030791 Ack=224530950 win=16740 Len=0
47	19.950000	192.168.10.77	192.168.100.3	TCP	4243 > ftp-data [ACK] Seq=930030791 Ack=224531966 win=16740 Len=0
48	20.083333	192.168.100.3	192.168.10.77	FTP-DATA	FTP Data: 508 bytes
49	20.083333	192.168.100.3	192.168.10.77	FTP-DATA	FTP Data: 60 bytes
50	20.083333	192.168.100.3	192.168.10.77	FTP-DATA	FTP Data: 508 bytes
51	20.083333	192.168.100.3	192.168.10.77	FTP-DATA	FTP Data: 420 bytes
52	20.083333	192.168.100.3	192.168.10.77	FTP-DATA	FTP Data: 508 bytes
53	20.083333	192.168.10.77	192.168.100.3	TCP	4243 > ftp-data [ACK] Seq=930030791 Ack=224532534 win=16740 Len=0
54	20.083333	192.168.10.77	192.168.100.3	TCP	4243 > ftp-data [ACK] Seq=930030791 Ack=224533462 win=16740 Len=0
55	20.183333	192.168.10.77	192.168.100.3	TCP	4243 > ftp-data [ACK] Seq=930030791 Ack=224533970 win=16232 Len=0
56	20.200000	192.168.100.3	192.168.10.77	FTP-DATA	FTP Data: 508 bytes
57	20.200000	192.168.100.3	192.168.10.77	FTP-DATA	FTP Data: 508 bytes
58	20.216667	192.168.100.3	192.168.10.77	FTP-DATA	FTP Data: 60 bytes
59	20.216667	192.168.100.3	192.168.10.77	FTP-DATA	FTP Data: 508 bytes
60	20.216667	192.168.10.77	192.168.100.3	TCP	4243 > ftp-data [ACK] Seq=930030791 Ack=224534986 win=16740 Len=0
61	20.216667	192.168.10.77	192.168.10.77	FTP-DATA	FTP Data: 508 bytes
62	20.216667	192.168.10.77	192.168.100.3	TCP	4243 > ftp-data [ACK] Seq=930030791 Ack=224535554 win=16740 Len=0

Copyright © 2005 Nortel Networks Limited - All Rights Reserved. Nortel, Nortel Networks, the Nortel logo, Globemark, and Contivity are trademarks of Nortel Networks Limited.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Limited.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Nortel Networks Technical Support on the web at: <http://www.nortel.com/support>

If after following this guide you are still having problems, please ensure you have carried out the steps exactly as in this document. If problems still persist, please contact Nortel Networks Technical Support (contact information is available online at: [http://www.nortel.com/cgi-bin/comments/comments.cgi?key=techsupport\\_cu](http://www.nortel.com/cgi-bin/comments/comments.cgi?key=techsupport_cu)).

We welcome your comments and suggestions on the quality and usefulness of this document. If you would like to leave a feedback please send your comments to: [CRCONT@nortel.com](mailto:CRCONT@nortel.com)

Author: Kristina Senkova