

## Re: Trouble accessing Outlook Web Access from behind firewall

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/8382.html>

---

**From:**

**Date:** 08/30/02

Date: Fri, 30 Aug 2002 22:31:59 +0200

Had a brainwave and found the culprit. When starting the firewall I also set up transparent HTTP proxy to Squid. This introduces the problem as Squid is a HTTP/1.0 proxy, not HTTP/1.1. Still working on a solution for this.

– Jan.

"Jan Klaverstijn" <[jan@klaverstijn.nl](mailto:jan@klaverstijn.nl)> schreef in bericht  
news:3d6f582e\$0\$21874\$1b62eedf@news.euronet.nl...

> *I run an iptables v1.2.6a firewall on Linux 2.4 to protect my adsl  
connected*

> *network.*

>

> *If I try to connect to Outlook Web Access on an external site from my  
WinXP*

> *box behind this firewall I get prompted for userid/password but never get*

> *authorized. The prompt reappears three times and then I am locked out. If*

**I**

> *shut down the firewall and just do basic masquerading it works fine. All*

> *rejected and dropped packets are logged, however I see nothing in my log*

> *related to this problem.*

>

> *Can anyone give me some clue as to what may be happening here? My firewall*

> *script is below.*

>

> *Regards, Jan.*

>

> *#!/bin/sh*

> *#*

> *#!/usr/local/sbin/firewall.iptables.devel*

> *#*

> *# Created by:*

> *# M.J. Prinsen – [dompie@mail.com](mailto:dompie@mail.com)*

> *#*

> *# <http://www.adsl4linux.nl>*

> *#*

> *#*

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> # $Id: firewall.iptables,v 1.13 2001/06/27 10:44:50 dompie Exp $
> #
> #
> ## -----
> ## READ THIS FIRST !!!
> ##
> ## This firewall is using a configuration file
> ## /etc/adslfirewall.conf for filling in some parameters.
> ## User specific services can also be set in this
> ## configuration file. DON'T EDIT THE SCRIPT FOR THIS.
> ##
> ## Please have a look at the configuration file !
> ## -----
> #
> #
> PATH=/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/bin:/usr/local/sbin
>
> # Set path to iptables
> export path_iptables="/usr/local/sbin/iptables"
>
> function testresult {
> let i=i+$1
> case $1 in
> '0')
> # echo -e "\033[40m\033[1;32mOK\033[0m"
> echo -e "OK"
> ;;
> '1')
> # echo -e "\033[40m\033[1;31mFailed\033[0m"
> echo -e "Failed"
> ;;
> '2')
> # echo -e "\033[40m\033[1;31mFatal Error: 2\033[0m"
> echo -e "Fatal Error: 2"
> ;;
> *)
> # echo -e "\033[40m\033[1;31mFatal Error: ?\033[0m"
> echo -e "Fatal Error: ?"
> ;;
> esac
> return $i
> }
>
>
> case "$1" in
>
> start)
> # ***** STARTING FIREWALL *****
> echo;
>
> datum=`date +%b %d %k:%M:%S`;
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> echo "$datum Starting firewall iptables ..." | tee -a /var/log/messages
> sleep 5
>
> # Define, check and read firewall configuration file
> FILE=/etc/adslfirewall.conf
> if [ -e $FILE ];
> then
> . $FILE
> else
> echo;
> echo "The file $FILE doesn't exist!"
> echo "The firewall is using this file for his configurationparameters."
> echo "Please check if the file is in place and readable for root."
> echo;
> exit;
> fi;
>
> #-----
> # Load kernel modules
> #-----
> # Insert modules if not compiled within the kernel
> if [ $load_modules = "y" ]; then
> # /sbin/insmod ip_tables
> # /sbin/insmod ip_conntrack
> /sbin/insmod ip_conntrack_ftp
> /sbin/insmod ip_queue
> # /sbin/insmod iptable_nat
> # /sbin/insmod iptable_filter
> # /sbin/insmod iptable_mangle
> /sbin/insmod ip_nat_ftp
> /sbin/insmod ip_nat_irc
> # /sbin/insmod ipt_iplimit
> # /sbin/insmod ipt_limit
> # /sbin/insmod ipt_state
> /sbin/insmod ipt_multiport
> /sbin/insmod ipt_mark
> # /sbin/insmod ipt_MASQUERADE
> # /sbin/insmod ipt_REJECT
> # /sbin/insmod ipt_REDIRECT
> # /sbin/insmod ipt_TOS
> /sbin/insmod ipt_MIRROR
> # /sbin/insmod ipt_LOG
> echo "Loading kernel modules ...";
> sleep 5
> fi;
>
>
> #-----
> # Initialize kernel
> #-----
>
```

## comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> if [ $initialize_kernel = "y" ]; then
> echo "Initializing kernel ..."
> # CRITICAL: Enable IP forwarding since it is disabled by default since
> if [ -e /proc/sys/net/ipv4/ip_forward ]; then
> echo 1 > /proc/sys/net/ipv4/ip_forward
> else
> echo "Uh oh: /proc/sys/net/ipv4/ip_forward does not exist"
> echo "(That may be a problem)"
> echo
> fi;
> sleep 5
>
> # Turn on source address verification in kernel
> if [ -e /proc/sys/net/ipv4/conf/all/rp_filter ]; then
> for interface in /proc/sys/net/ipv4/conf/*/rp_filter; do
> echo 1 > $interface;
> done
> fi;
>
> # Disable ICMP Redirect acceptance
> if [ -e /proc/sys/net/ipv4/conf/all/accept_redirects ]; then
> for interface in /proc/sys/net/ipv4/conf/*/accept_redirects; do
> echo 0 > $interface;
> done
> fi;
>
> # Disable ICMP send_redirect
> if [ -e /proc/sys/net/ipv4/conf/all/send_redirects ]; then
> for interface in /proc/sys/net/ipv4/conf/*/send_redirects; do
> echo 0 > $interface;
> done
> fi;
>
> # Don't accept source routed packets
> if [ -e /proc/sys/net/ipv4/conf/all/accept_source_route ]; then
> for interface in /proc/sys/net/ipv4/conf/*/accept_source_route; do
> echo 0 > $interface;
> done
> fi;
>
> # Log spoofed packets, source routed packets, redirect packets
> if [ -e /proc/sys/net/ipv4/conf/all/log_martians ]; then
> for interface in /proc/sys/net/ipv4/conf/*/log_martians; do
> echo 1 > $interface;
> done
> fi;
>
> # Turn on syn cookies protection in kernel
> if [ -e /proc/sys/net/ipv4/tcp_syncookies ]; then
> echo 1 > /proc/sys/net/ipv4/tcp_syncookies
> fi;
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
>
> # ICMP Broadcasting protection
> if [ -e /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts ]; then
> echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
> fi;
>
> # ICMP Dead Error Messages protection
> if [ -e /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses ]; then
> echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
> fi;
>
> # Enable automatic IP defragmenting
> if [ -e /proc/sys/net/ipv4/ip_always_defrag ]; then
> echo 1 > /proc/sys/net/ipv4/ip_always_defrag
> fi;
>
> # Turn on dynamic TCP/IP address hacking ... turn off with echo 0 > ...
> if [ -e /proc/sys/net/ipv4/ip_dynaddr ]; then
> echo 1 > /proc/sys/net/ipv4/ip_dynaddr
> fi;
>
> # Set the maximum number of connections to track. (Kernel Default: 2048)
> if [ -e /proc/sys/net/ipv4/ip_conntrack_max ]; then
> echo 4096 > /proc/sys/net/ipv4/ip_conntrack_max
> fi
>
> # Enable the LooseUDP patch which some Internet-based games require
> #
> # If you are trying to get an Internet game to work through your IP MASQ
> # box,
> # and you have set it up to the best of your ability without it working,
> # try
> # enabling this option (delete the "#" character). This option is
disabled
> # by default due to possible internal machine UDP port scanning
> # vulnerabilities.
> # Turned off by default ... turn on with echo 1 > ...
> if [ -e /proc/sys/net/ipv4/ip_masq_udp_dloose ]; then
> echo 0 > /proc/sys/net/ipv4/ip_masq_udp_dloose
> fi;
>
> fi;
>
> #-----
> # Initialisatie
> #-----
>
> # Check if ppp+ is up
> check=`/sbin/ifconfig -a | grep ppp`
> if [ -z "$check" ]
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> then
> echo "You don't have a working connection, please check this before
bringing
> up the firewall!"
> sleep 5
> exit 2;
> else
> echo "Check ppp ... ok ... continue"
> sleep 5
> fi;
>
>
>
#####
> #
>
>
#-----
> # Flush and clearing rulez and setting default policies
>
#-----
> $path_iptables -F &&
> $path_iptables -X &&
> $path_iptables -Z &&
> $path_iptables -t nat -F &&
> $path_iptables -t nat -X &&
> $path_iptables -t nat -Z &&
> $path_iptables -t mangle -F &&
> $path_iptables -t mangle -X &&
> $path_iptables -t mangle -Z
> err=`testresult $?`
> i=$?
> echo "Flushing and clearing rules ...$err";
>
> $path_iptables -P INPUT DROP &&
> $path_iptables -P OUTPUT DROP &&
> $path_iptables -P FORWARD DROP &&
> $path_iptables -t nat -P POSTROUTING ACCEPT &&
> $path_iptables -t nat -P PREROUTING ACCEPT &&
> $path_iptables -t mangle -P OUTPUT ACCEPT &&
> $path_iptables -t mangle -P PREROUTING ACCEPT &&
>
> # Creating new chain (LDROP = LOG & DROP) for logging
> $path_iptables -N LDROP &&
>
> # Creating new chain (CHECK_FLAGS) for checking the flags of incoming
> packets
> $path_iptables -N CHECK_FLAGS &&
> $path_iptables -F CHECK_FLAGS
> err=`testresult $?`
> i=$?
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> echo "Setting default policies ... $err";
>
> #-----
> # Loopback settings
> #-----
> $path_iptables -A INPUT -i lo -j ACCEPT &&
> $path_iptables -A OUTPUT -o lo -j ACCEPT &&
> $path_iptables -A INPUT -i $ext_if -d 127.0.0.0/8 -j LDROP
> err=`testresult $?`
> i=$?
> echo "Enabling loopback settings ... $err";
>
> #-----
> # Modem traffic
> #-----
> # Refuse spoofing
> $path_iptables -A INPUT -i $ext_if -s $modem_net -j LDROP &&
>
> # Only traffic between modem and server is welcome
> $path_iptables -A INPUT -i $modem_eth -s $modem_ip -d $modem_ethip -j
ACCEPT
> &&
> $path_iptables -A OUTPUT -o $modem_eth -s $modem_ethip -d $modem_ip -j
ACCEPT &&
>
> # View your modemsettings with your browser via http://10.0.0.138 from
every
> # computer on your LAN
> $path_iptables -t nat -A POSTROUTING -s $local_net -d $modem_ip -j
MASQUERADE
> err=`testresult $?`
> i=$?
> echo "Initializing modemrules ... $err";
>
> #-----
> # Local traffic
> #-----
> # Assemble before forwarding
> $path_iptables -A OUTPUT -f -o $local_if -j LDROP &&
>
> # Refuse spoofing
> $path_iptables -A INPUT -i $ext_if -s $local_net -j LDROP &&
>
> # Everything else is fine
> $path_iptables -A INPUT -i $local_if -s $local_net -j ACCEPT &&
> $path_iptables -A OUTPUT -o $local_if -d $local_net -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Enabling local traffic ... $err";
>
> #-----
```

```
> # Masquerade
> #-----
> # Higher ports needed to accept incoming/outgoing calls
> # Any traffic from masqueraded machines/server accepted
> # Reject any traffic not started by masqueraded machine/server
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
> $unpriv_ports ! --syn -m state --state NEW -j LDROP &&
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
> $unpriv_ports ! --syn -j ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport
> $unpriv_ports -d any/0 -j ACCEPT &&
>
> # Check if UDP connections are needed
> $path_iptables -A INPUT -p udp -i $ext_if -s any/0 -d $ext_ip --dport
> $unpriv_ports -j ACCEPT &&
> $path_iptables -A OUTPUT -p udp -o $ext_if -s $ext_ip --sport
> $unpriv_ports -d any/0 -j ACCEPT &&
>
> # All local traffic is masqueraded externally
> $path_iptables -t nat -A POSTROUTING -o $ext_if -s $local_net -j
MASQUERADE
> &&
>
> # Only forward packages for our subnet
> # Forward internal to external and external to internal net traffic
> $path_iptables -A FORWARD -s $local_net -j ACCEPT &&
> $path_iptables -A FORWARD -d $local_net -j ACCEPT &&
>
> # Take advantage of connection tracking
> $path_iptables -A INPUT -p tcp -i $ext_if -d $ext_ip -m state --state
> ESTABLISHED,RELATED -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Setting masquerading ... $err";
>
> #-----
> # DHCP server communicatie
> #-----
> # Open port 67 (bootps) for DHCP server
> if [ $dhcp = "y" ]; then
> $path_iptables -A INPUT -p udp -i $local_if -s any/0 --sport 68 -d
> $broadcast --dport 67 -j ACCEPT &&
> $path_iptables -A OUTPUT -p udp -o $local_if -s $local_ip -d $broadcast -j
> ACCEPT &&
>
> $path_iptables -A INPUT -p udp -i $local_if --dport bootps --sport
bootpc -j
> ACCEPT &&
> $path_iptables -A OUTPUT -p udp -o $local_if --sport bootps --dport
> bootpc -j ACCEPT
> err=`testresult $?`
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> i=$?
> echo "Setup DHCP ... $err";
> fi;
>
>
> #-----
> # This is all generic protection against spoofing
> #-----
> if [ $spoofing_protection = "y" ]; then
> # Block Packets with Stuffed Routing
> $path_iptables -A INPUT -s 0.0.0.0 -j LDROP &&
> $path_iptables -A OUTPUT -s 0.0.0.0 -j LDROP &&
> $path_iptables -A INPUT -s 255.255.255.255 -j LDROP &&
> $path_iptables -A OUTPUT -s 255.255.255.255 -j LDROP &&
>
> # Block Fragmented Packets
> $path_iptables -A INPUT -f -m limit --limit 5/minute -j LDROP &&
>
> # Block all reserved private IP addresses
> $path_iptables -A INPUT -i $ext_if -s $class_a -j LDROP &&
> $path_iptables -A INPUT -i $ext_if -s $class_b -j LDROP &&
> $path_iptables -A INPUT -i $ext_if -s $class_c -j LDROP &&
> $path_iptables -A INPUT -i $ext_if -s $class_d -j LDROP &&
> $path_iptables -A INPUT -i $ext_if -s $class_e -j LDROP &&
>
> # Block all ip addresses reserved by IANA (for the time being)
> # this changes regularly, see
> http://www.iana.org/assignments/ipv4-address-space
> # Updated 25 May 2001
>
> RESERVED_NET="
> 0.0.0.0/8 1.0.0.0/8 2.0.0.0/8 \
> 5.0.0.0/8 \
> 7.0.0.0/8 \
> 23.0.0.0/8 \
> 27.0.0.0/8 \
> 31.0.0.0/8 \
> 36.0.0.0/8 37.0.0.0/8 \
> 39.0.0.0/8 \
> 41.0.0.0/8 42.0.0.0/8 \
> 58.0.0.0/8 59.0.0.0/8 60.0.0.0/8 \
> 68.0.0.0/8 69.0.0.0/8 70.0.0.0/8 71.0.0.0/8 72.0.0.0/8 73.0.0.0/8 \
> 74.0.0.0/8 75.0.0.0/8 76.0.0.0/8 77.0.0.0/8 78.0.0.0/8 79.0.0.0/8 \
> 82.0.0.0/8 83.0.0.0/8 84.0.0.0/8 85.0.0.0/8 86.0.0.0/8 87.0.0.0/8 \
> 88.0.0.0/8 89.0.0.0/8 90.0.0.0/8 91.0.0.0/8 92.0.0.0/8 93.0.0.0/8 \
> 94.0.0.0/8 \
> 95.0.0.0/8 96.0.0.0/8 97.0.0.0/8 98.0.0.0/8 99.0.0.0/8 100.0.0.0/8 \
> 101.0.0.0/8 \
> 102.0.0.0/8 103.0.0.0/8 104.0.0.0/8 105.0.0.0/8 106.0.0.0/8 107.0.0.0/8 \
> 108.0.0.0/8 109.0.0.0/8 110.0.0.0/8 111.0.0.0/8 112.0.0.0/8 113.0.0.0/8 \
> 114.0.0.0/8 115.0.0.0/8 116.0.0.0/8 117.0.0.0/8 118.0.0.0/8 119.0.0.0/8 \
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> 120.0.0.0/8 121.0.0.0/8 122.0.0.0/8 123.0.0.0/8 124.0.0.0/8 125.0.0.0/8 \  
> 126.0.0.0/8 127.0.0.0/8 \  
> 197.0.0.0/8 \  
> 219.0.0.0/8 220.0.0.0/8 221.0.0.0/8 222.0.0.0/8 223.0.0.0/8 \  
> 224.0.0.0/8 225.0.0.0/8 226.0.0.0/8 227.0.0.0/8 228.0.0.0/8 229.0.0.0/8 \  
> 230.0.0.0/8 231.0.0.0/8 232.0.0.0/8 233.0.0.0/8 234.0.0.0/8 235.0.0.0/8 \  
> 236.0.0.0/8 237.0.0.0/8 238.0.0.0/8 239.0.0.0/8 \  
> 240.0.0.0/8 241.0.0.0/8 242.0.0.0/8 243.0.0.0/8 244.0.0.0/8 245.0.0.0/8 \  
> 246.0.0.0/8 247.0.0.0/8 248.0.0.0/8 249.0.0.0/8 250.0.0.0/8 251.0.0.0/8 \  
> 252.0.0.0/8 253.0.0.0/8 254.0.0.0/8 255.0.0.0/8"  
>  
> a=0  
> for NET in $RESERVED_NET; do  
> $path_iptables -A INPUT -s $NET -j LDROP  
> if [ $? != 0 ]  
> then  
> a=1  
> break;  
> fi  
> done;  
> err=`testresult $a`  
> let i=i+$?  
> echo "Setting up generic protection against spoofing ... $err"  
>  
> fi;  
>  
>  
> #-----  
> # Refusing some common ports  
> #-----  
> # Especially necessary to set this feature when opening ALL unpriv_ports  
> # for instance due to ICQ filetransfer.  
> # Avoid ports subject to protocol & system administration problems.  
>  
> if [ $refuse_common_ports = "y" ]; then  
>  
> # SOCKS: disable incoming connections on port 1080  
> # Openwindows: disable incoming connections on port 2000  
> # NFS: disable incoming connections to port 2049  
> # SQUID: disable incoming connections on port 3128  
> # Xwindows: disable incoming connections on ports 6000:6063  
> # Block IRC on ports 6665:6669  
> # WEBPROXY: disable incoming connections on port 8080  
>  
>  
> common_ports_refused="1080 2000 2049 3128 6000:6063 6665:6669 8080"  
> a=0  
> for common_ports in $common_ports_refused;  
> do  
> $path_iptables -A INPUT -p tcp -i $ext_if --dport $common_ports -j LDROP  
&&
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> $path_iptables -A OUTPUT -p tcp -o $ext_if --dport $common_ports -j LDROP
&&
> $path_iptables -A INPUT -p udp -i $ext_if --dport $common_ports -j LDROP
&&
> $path_iptables -A OUTPUT -p udp -o $ext_if --dport $common_ports -j LDROP
> if [ $? != 0 ]
> then
> a=1
> break;
> fi
> done;
> err=`testresult $a`
> i=$?
> echo "Refuse connection to common known ports ... $err";
> fi;
>
>
> #-----
> # Refusing some Trojan-ports
> #-----
> # Especially necessary to set this feature when opening ALL unpriv_ports
> # for instance due to ICQ filetransfer.
> # Trojan-ports: disable incoming connections to common trojan ports
>
> if [ $block_trojans = "y" ]; then
>
> # Block Subseven (1.7/1.9) 1243 / 6711:6713
> # Block Backdoor-G and Subseven (2.X) 1999 / 6776 / 27374
> # Block NetBus 12345:12346
> # Block NetBus 2 Pro 20034
> # Block Stacheldraht 16660 / 60001 / 65000
> # Block Back Orifice, Deep BO 31337:31338
> # Block Back Orifice 2K 54320:54321
> # Block Trinity v3\n 33270
> # Block Trin00 1524 / 27444 / 27665 / 31335
> # Block Cheeseworm 10008
>
>
> trojan_ports="1243 6711:6713 1999 6776 27374 12345:12346 20034 16660 60001
\
> 65000 31337:31338 54320:54321 33270 1524 27444 27665 31335 10008"
> a=0
> for trojans in $trojan_ports;
> do
> $path_iptables -A INPUT -p tcp -i $ext_if --dport $trojans -j LDROP &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if --dport $trojans -j LDROP &&
> $path_iptables -A INPUT -p udp -i $ext_if --dport $trojans -j LDROP &&
> $path_iptables -A OUTPUT -p udp -o $ext_if --dport $trojans -j LDROP
> if [ $? != 0 ]
> then
> a=1
```

```
> break;
> fi
> done;
> err=`testresult $a`
> i=$?
> echo "Block Trojans ... $err";
>
> fi;
>
>
> #-----
> # Refusing some common scans and attacks
> #-----
> # Especially necessary to set this feature when opening ALL unpriv_ports
> # for instance due to ICQ filetransfer.
> # Check flags incoming packets
> if [ $check_flags_packets = "y" ]; then
>
> # NMAP FIN/URG/PSH - XMAS - scan
> $path_iptables -A CHECK_FLAGS -p tcp --tcp-flags ALL FIN,URG,PSH -m limit \
> --limit 5/minute -j LOG --log-level notice --log-prefix "NMAP-XMAS: " &&
> $path_iptables -A CHECK_FLAGS -p tcp --tcp-flags ALL FIN,URG,PSH -j DROP
&&
>
> # SYN/RST - scan
> $path_iptables -A CHECK_FLAGS -p tcp --tcp-flags SYN,RST SYN,RST -m limit \
> --limit 5/minute -j LOG --log-level notice --log-prefix "SYN/RST: " &&
> $path_iptables -A CHECK_FLAGS -p tcp --tcp-flags SYN,RST SYN,RST -j DROP
&&
>
> # SYN/FIN -- scan(probably)
> $path_iptables -A CHECK_FLAGS -p tcp --tcp-flags SYN,FIN SYN,FIN -m limit \
> --limit 5/minute -j LOG --log-level notice --log-prefix "SYN/FIN: " &&
> $path_iptables -A CHECK_FLAGS -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP
&&
>
> # FIN - scan
> $path_iptables -A CHECK_FLAGS -p tcp --tcp-flags ALL FIN -m limit \
> --limit 5/minute -j LOG --log-level notice --log-prefix "FIN: " &&
> $path_iptables -A CHECK_FLAGS -p tcp --tcp-flags ALL FIN -j DROP &&
>
> # ALL/ALL - scan
> $path_iptables -A CHECK_FLAGS -p tcp --tcp-flags ALL ALL -m limit \
> --limit 5/minute -j LOG --log-level notice --log-prefix "ALL/ALL: " &&
> $path_iptables -A CHECK_FLAGS -p tcp --tcp-flags ALL ALL -j DROP &&
>
> # NULL - scan
> $path_iptables -A CHECK_FLAGS -p tcp --tcp-flags ALL NONE -m limit \
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> --limit 5/minute -j LOG --log-level notice --log-prefix "NULL: " &&
> $path_iptables -A CHECK_FLAGS -p tcp --tcp-flags ALL NONE -j DROP &&
>
> # Check TCP packets coming in on the external interface for wierd flags
> $path_iptables -A INPUT -i $ext_if -p tcp -j CHECK_FLAGS &&
> # Check TCP packets going out on the external interface for wierd flags.
> $path_iptables -A OUTPUT -o $ext_if -p tcp -j CHECK_FLAGS
> err=`testresult $?`
> i=$?
> echo "Setup checking flags incoming packets ... $err";
> fi;
>
>
> #-----
> # ICMP settings
> #-----
>
> # Only accept pings from www.watchmyserver.com (195.179.115.45)
> # With protection against ping of death
> # icmp trafic
> # 0 = echo-reply needed by ping
> # 3 = destination-unreachable needed by any TCP/UDP trafic
> # 5 = redirect needed by routing if not running routing daemon
> # 8 = echo-request needed by ping
> #11 = time-exceeded needed by traceroute
>
> if [ $accept_pings = "y" ]; then
> $path_iptables -A INPUT -i $ext_if -p icmp --icmp-type 0 -s any/0 -d
> $ext_ip -m limit --limit 1/s -j ACCEPT &&
> $path_iptables -A INPUT -i $ext_if -p icmp --icmp-type 3 -s any/0 -d
> $ext_ip -m limit --limit 1/s -j ACCEPT &&
> $path_iptables -A INPUT -i $ext_if -p icmp --icmp-type 8 -s any/0 -d
> $ext_ip -m limit --limit 1/s -j ACCEPT &&
> $path_iptables -A INPUT -i $ext_if -p icmp --icmp-type 11 -s any/0 -d
> $ext_ip -m limit --limit 1/s -j ACCEPT &&
>
> $path_iptables -A OUTPUT -o $ext_if -p icmp --icmp-type 3 -s $ext_ip -d
> any/0 -m limit --limit 1/s -j ACCEPT &&
> $path_iptables -A OUTPUT -o $ext_if -p icmp --icmp-type 8 -s $ext_ip -d
> any/0 -m limit --limit 1/s -j ACCEPT &&
> $path_iptables -A OUTPUT -o $ext_if -p icmp --icmp-type 0 -s $ext_ip -d
> any/0 -m limit --limit 1/s -j ACCEPT &&
> $path_iptables -A OUTPUT -o $ext_if -p icmp --icmp-type 11 -s $ext_ip -d
> any/0 -m limit --limit 1/s -j ACCEPT &&
>
> # Accept redirect icmp-packets
> $path_iptables -A INPUT -i $ext_if -p icmp --icmp-type 5 -s any/0 -d
> $ext_ip -m limit --limit 1/s -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Set accept pings ... $err";
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
>
> else
> $path_iptables -A INPUT -i $ext_if -p icmp --icmp-type 0 -s any/0 -d
> $ext_ip -m limit --limit 1/s -j ACCEPT &&
> $path_iptables -A INPUT -i $ext_if -p icmp --icmp-type 3 -s any/0 -d
> $ext_ip -m limit --limit 1/s -j ACCEPT &&
> $path_iptables -A INPUT -i $ext_if -p icmp --icmp-type 8 -s
> 195.179.115.45 -d $ext_ip -m limit --limit 1/s -j ACCEPT &&
> $path_iptables -A INPUT -i $ext_if -p icmp --icmp-type 11 -s any/0 -d
> $ext_ip -m limit --limit 1/s -j ACCEPT &&
>
> $path_iptables -A OUTPUT -o $ext_if -p icmp --icmp-type 3 -s $ext_ip -d
> any/0 -m limit --limit 1/s -j ACCEPT &&
> $path_iptables -A OUTPUT -o $ext_if -p icmp --icmp-type 8 -s $ext_ip -d
> any/0 -m limit --limit 1/s -j ACCEPT &&
> $path_iptables -A OUTPUT -o $ext_if -p icmp --icmp-type 0 -s $ext_ip -d
> 195.179.115.45 -m limit --limit 1/s -j ACCEPT &&
> $path_iptables -A OUTPUT -o $ext_if -p icmp --icmp-type 11 -s $ext_ip -d
> 195.179.115.45 -m limit --limit 1/s -j ACCEPT &&
>
> # Deny redirect icmp-packets
> $path_iptables -A INPUT -i $ext_if -p icmp --icmp-type 5 -s any/0 -d
> $ext_ip -j LDROP
> err=`testresult $?`
> i=$?
> echo "Set no pings accepted ... $err";
> fi;
>
>
>
#-----
> # Mangles the TOS on standard ports so they get priority in routers
>
#-----
> # TOS table
> # Options:
> # Normal-Service = 0 (0x00)
> # Minimize-Cost = 2 (0x02)
> # Maximize-Reliability = 4 (0x04)
> # Maximize-Throughput = 8 (0x08)
> # Minimize-Delay = 16 (0x10)
>
>
> if [ $mangle_tos = "y" ]; then
> # ToS: Client Applications; data => tos_client
> # Most of these are the RFC 1060/1349 suggested TOS values, yours might
> vary.
> # To view mangle table, type: iptables -L -t mangle
>
> # Mangle values of packets created locally.
> $path_iptables -t mangle -A OUTPUT -p tcp --dport 20 -j TOS --set-tos
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> Maximize-Throughput &&
> $path_iptables -t mangle -A OUTPUT -p tcp --dport 21 -j TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A OUTPUT -p tcp --dport 22 -j TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A OUTPUT -p tcp --dport 23 -j TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A OUTPUT -p tcp --dport 25 -j TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A OUTPUT -p udp --dport 53 -j TOS --set-tos
> Maximize-Throughput &&
> $path_iptables -t mangle -A OUTPUT -p tcp --dport 67 -j TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A OUTPUT -p tcp --dport 80 -j TOS --set-tos
> Maximize-Throughput &&
> $path_iptables -t mangle -A OUTPUT -p tcp --dport 110 -j TOS --set-tos
> Maximize-Throughput &&
> $path_iptables -t mangle -A OUTPUT -p tcp --dport 113 -j TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A OUTPUT -p tcp --dport 123 -j TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A OUTPUT -p tcp --dport 143 -j TOS --set-tos
> Maximize-Throughput &&
> $path_iptables -t mangle -A OUTPUT -p tcp --dport 443 -j TOS --set-tos
> Maximize-Throughput &&
> $path_iptables -t mangle -A OUTPUT -p tcp --dport 993 -j TOS --set-tos
> Maximize-Throughput &&
> $path_iptables -t mangle -A OUTPUT -p tcp --dport 995 -j TOS --set-tos
> Maximize-Throughput &&
> $path_iptables -t mangle -A OUTPUT -p tcp --dport 1080 -j TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A OUTPUT -p tcp --dport 6000:6063 -j
TOS --set-tos
> Maximize-Throughput &&
>
> # Rules to mangle TOS values of packets routed through the firewall
> $path_iptables -t mangle -A PREROUTING -p tcp --dport 20 -j TOS --set-tos
> Maximize-Throughput &&
> $path_iptables -t mangle -A PREROUTING -p tcp --dport 21 -j TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A PREROUTING -p tcp --dport 22 -j TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A PREROUTING -p tcp --dport 23 -j TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A PREROUTING -p tcp --dport 25 -j TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A PREROUTING -p udp --dport 53 -j TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A PREROUTING -p tcp --dport 67 -j TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A PREROUTING -p tcp --dport 80 -j TOS --set-tos
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> Maximize-Throughput &&
> $path_iptables -t mangle -A PREROUTING -p tcp --dport 110 -j TOS --set-tos
> Maximize-Throughput &&
> $path_iptables -t mangle -A PREROUTING -p tcp --dport 113 -j TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A PREROUTING -p tcp --dport 123 -j TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A PREROUTING -p tcp --dport 143 -j TOS --set-tos
> Maximize-Throughput &&
> $path_iptables -t mangle -A PREROUTING -p tcp --dport 443 -j TOS --set-tos
> Maximize-Throughput &&
> $path_iptables -t mangle -A PREROUTING -p tcp --dport 993 -j TOS --set-tos
> Maximize-Throughput &&
> $path_iptables -t mangle -A PREROUTING -p tcp --dport 995 -j TOS --set-tos
> Maximize-Throughput &&
> $path_iptables -t mangle -A PREROUTING -p tcp --dport 1080 -j
TOS --set-tos
> Minimize-Delay &&
> $path_iptables -t mangle -A PREROUTING -p tcp --dport 6000:6063 -j
TOS --set-tos Maximize-Throughput
> err=`testresult $?`
> i=$?
> echo "Setup mangling TOS ... $err";
> fi;
>
>
> #-----
> # ICQ filetransfer / Syn-flood protection
> #-----
> # Unfortunately ICQ uses the whole unpriv_port range for client to client
> connections (filetransfer)
> # Enabling this feature will open ALL unpriv_ports. Hackers are then able
to
> establish a
> # connection to these ports. However you are prevented from DoS (Denial of
> Service) attacks.
> # --limit followed by a number; specifies the maximum average number of
> matches to allow per second.
> if [ $icq_filetransfer_all = "y" ]; then
> $path_iptables -A INPUT -p tcp -i $ext_if -d $ext_ip --dport
> $unpriv_ports -m limit --limit 1/s --syn -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Enabling ICQ filetransfer ... !!! Caution, opens ALL unpriv_ports
!!!
> ... $err";
> fi;
>
> # Restricted ICQ filetransfer based on IP-address
> if [ $icq_filetransfer_friends = "y" ]; then
> a=0
```

```
> for icq_ip in $icq_friends;
> do
> $path_iptables -A INPUT -p tcp -i $ext_if -s $icq_ip --sport
> $unpriv_ports -d $ext_ip --dport $unpriv_ports -j ACCEPT
> if [ $? != 0 ]
> then
> a=1
> break;
> fi
> done;
> err=`testresult $a`
> let i=i+$?
> echo "Enable restricted ICQ filetransfer ... $err";
> fi;
>
>
> #-----
> # FTP-server
> #-----
> if [ $ftp_active = "y" -o $ftp_passive = "y" ]; then
> # Open port 21 (ftp) for FTP-server
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
ftp -m
> state --state NEW,ESTABLISHED -j ACCEPT
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport ftp -d
any/0 -m state --state ESTABLISHED,RELATED -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Opening port 21 for ftp ... $err";
> fi;
>
> if [ $ftp_active = "y" ]; then
> # Open port 20 (ftp-data) for active FTP-server
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
> ftp-data -m state --state ESTABLISHED,RELATED ! --syn -j ACCEPT
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport ftp-data -d
any/0 -m state --state ESTABLISHED,RELATED -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Opening port 20 for datatransfer active FTP ... $err";
> fi;
>
> if [ $ftp_passive = "y" ]; then
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
> $unpriv_ports -m state --state ESTABLISHED,RELATED -j ACCEPT
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport
> $unpriv_ports -d any/0 -m state --state ESTABLISHED,RELATED -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Opening unpriv. ports for datatransfer passive FTP ... $err";
> fi;
```

```
>
>
> #-----
> # SSH server and client traffic
> #-----
> # Any traffic to/from ssh daemon permitted
> if [ $ssh = "y" ]; then
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
ssh -j
> ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport ssh -d any/0
> ! --syn -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Enable SSH ... $err";
> fi;
>
>
> #-----
> # Telnet
> #-----
> # Open port 23 (telnet) for Telnet
> if [ $telnet = "y" ]; then
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
> telnet -j ACCEPT
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport telnet -d
> any/0 ! --syn -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Sustain Telnet ... $err";
> fi;
>
>
> #-----
> # SMTP-server
> #-----
> # Open port 25 (smtp) for SMTP-server
> if [ $smtp = "y" ]; then
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
> smtp -j ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport smtp -d
any/0
> ! --syn -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Opening SMTP for mailserver ... $err";
> fi;
>
>
> #-----
> # DNS-server
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> #-----
> # Open port 53 (domain) for DNS-server
> if [ $dns = "y" ]; then
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
> domain -j ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport domain -d
> any/0 ! --syn -j ACCEPT &&
> $path_iptables -A INPUT -p udp -i $ext_if -s any/0 -d $ext_ip --dport
> domain -j ACCEPT &&
> $path_iptables -A OUTPUT -p udp -o $ext_if -s $ext_ip --sport domain -d
> any/0 -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Enable DNS ... $err";
> fi;
>
>
> #-----
> # Apache - webservice
> #-----
> # Open port 80 (http) for webservice
> if [ $http = "y" ]; then
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
> http -j ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport http -d
any/0
> ! --syn -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Give access to webservice ... $err"
> fi;
>
> # Open poort 443 (https) for webservice
> if [ $https = "y" ]; then
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
> https -j ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport https -d
any/0
> ! --syn -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Setup SSL ... $err";
> fi;
>
>
> #-----
> # POP3-server
> #-----
> # Open port 110 (pop3) for POP3-server
> if [ $pop3 = "y" ]; then
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> pop3 -j ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport pop3 -d
any/0
> ! --syn -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Open POP3 connection ... $err";
> fi;
>
> # Open port 995 (pop3s) for POP3-server over SSL
> if[ $pop3s = "y" ]; then
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
pop3s -j ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport pop3s -d
any/0
> ! --syn -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Open POP3 over SSL ... $err";
> fi;
>
>
> #-----
> # Auth-server (ident)
> #-----
> # Open port 113 (auth/ident) for ident-server
> # On some distributions "auth" needs to be replaced by "ident"
> if[ $auth = "y" ]; then
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
auth -j ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport auth -d
any/0
> ! --syn -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Enable Auth ... $err";
>
> else
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
auth -j REJECT --reject-with tcp-reset &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport auth -d
any/0
> ! --syn -j REJECT --reject-with tcp-reset
> err=`testresult $?`
> i=$?
> echo "Reject instead of drop Auth requests ... $err";
> fi;
>
>
>
>
#-----
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> ---
> # NTP: Allow external computers to connect to the Linux server ITSELF for
> # NTP (time) updates -----> ntp.xs4all.nl = 194.109.6.65 = ntp_ip
>
#-----
> ---
> # Open port 123 (ntp) for NTP
> if [ $ntp_tcp = "y" ]; then
> a=0
> for ntp_address in $ntp_ip; do
> $path_iptables -A INPUT -p tcp -i $ext_if -s $ntp_address --sport ntp -d
> $ext_ip --dport ntp -j ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport ntp -d
> $ntp_address --dport ntp -j ACCEPT
> if [ $? != 0 ]
> then
> a=1
> break;
> fi
> done;
> err=`testresult $a`
> let i=i+$?
> echo "Open tcp-protocol timeserver ... $err";
> fi;
>
> if [ $ntp_udp = "y" ]; then
> a=0
> for ntp_address in $ntp_ip; do
> $path_iptables -A INPUT -p udp -i $ext_if -s $ntp_address --sport ntp -d
> $ext_ip --dport ntp -j ACCEPT &&
> $path_iptables -A OUTPUT -p udp -o $ext_if -s $ext_ip --sport ntp -d
> $ntp_address --dport ntp -j ACCEPT
> if [ $? != 0 ]
> then
> a=1
> break;
> fi;
> done;
> err=`testresult $a`
> let i=i+$?
> echo "Open udp-protocol timeserver ... $err";
> fi;
>
>
> #-----
> # IMAP-server
> #-----
> # Open port 143 (imap) for IMAP-server
> if [ $imap = "y" ]; then
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
> imap -j ACCEPT &&
```

## comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport imap -d
any/0
> ! --syn -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Open IMAP connection ... $err";
> fi;
>
> # Open port 993 (imaps) for IMAP-server over SSL
> if[ $imaps = "y" ]; then
>
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
> imaps -j ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport imaps -d
any/0
> ! --syn -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Open IMAP over SSL ... $err";
> fi;
>
>
> #-----
> # Webmin-server
> #-----
> # Open port 10000 (webmin) for Webmin-server
> if[ $webmin = "y" ]; then
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
> 10000 -j ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport 10000 -d
any/0
> ! --syn -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Enable Webmin ... $err";
>
> else
> $path_iptables -A INPUT -p tcp -i $ext_if -s any/0 -d $ext_ip --dport
> 10000 -j LDROP &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport 10000 -d
> any/0 -j LDROP &&
> $path_iptables -A INPUT -p udp -i $ext_if -s any/0 -d $ext_ip --dport
> 10000 -j LDROP &&
> $path_iptables -A OUTPUT -p udp -o $ext_if -s $ext_ip --sport 10000 -d
> any/0 -j LDROP
> err=`testresult $?`
> i=$?
> echo "Disable Webmin ... $err";
> fi;
>
>
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> #-----
> # VNC-server
> #-----
> # It is more secure to establish a VNC-connection with Linux server via a
> SSH-tunnel
> # Establish an unencrypted VNC-connection with Linux server
> # Default display :1
> if [ $vnc_with_server = "y" ]; then
> $path_iptables -A INPUT -p tcp -i $ext_if -d $ext_ip --dport 5901 -m
> limit --limit 1/s --syn -j ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport 5901 -m
> limit --limit 1/s ! --syn -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Setup routing VNC to server ... $err";
>
> else
>
> $path_iptables -A INPUT -p tcp -i $ext_if -d $ext_ip --dport 5901 -j LDROP
> &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport 5901 -j
LDROP
> err=`testresult $?`
> i=$?
> echo "Disable routing VNC to server ... $err";
> fi;
>
> # Establish VNC-connection with masqueraded machine
> # Connect to port 5902 on Linux server --> routed to port 5910 on client
> machine where VNC is listening
> if [ $vnc_with_masq_machine = "y" ]; then
> $path_iptables -A INPUT -p tcp -i $ext_if -d $ext_ip --dport 5902 -m
> limit --limit 1/s --syn -j ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s $ext_ip --sport 5902 -m
> limit --limit 1/s ! --syn -j ACCEPT &&
> $path_iptables -t nat -A PREROUTING -p tcp -d $ext_ip --dport 5902 -j
> DNAT --to $masq_machine_ip:5910 &&
> $path_iptables -t nat -A POSTROUTING -p tcp -d $masq_machine_ip --dport
> 5910 -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Setup routing VNC to masq. machine ... $err";
> fi;
>
>
> #-----
> # ABN Amro Homenet
> #-----
> if [ $abnamro = "y" ]; then
> $path_iptables -A INPUT -p tcp -i $ext_if -s viaebt.eb.abnamro.com -d
> $ext_ip -j ACCEPT &&
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s viaebt.eb.abnamro.com -d
> $ext_ip -j ACCEPT &&
>
> $path_iptables -A INPUT -p tcp -i $ext_if -s viaebt1.eb.abnamro.com -d
> $ext_ip -j ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s viaebt1.eb.abnamro.com -d
> $ext_ip -j ACCEPT &&
>
> $path_iptables -A INPUT -p tcp -i $ext_if -s IIGPROD1.eb.abnamro.com -d
> $ext_ip -j ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s IIGPROD1.eb.abnamro.com -d
> $ext_ip -j ACCEPT &&
>
> $path_iptables -A INPUT -p tcp -i $ext_if -s IIGPROD2.eb.abnamro.com -d
> $ext_ip -j ACCEPT &&
> $path_iptables -A OUTPUT -p tcp -o $ext_if -s IIGPROD2.eb.abnamro.com -d
> $ext_ip -j ACCEPT
> err=`testresult $?`
> i=$?
> echo "Enable rules for HomeNet ... $err";
> fi;
>
>
> #-----
> # Private firewall rules
> #-----
> if [ $private_rules = "y" ]; then
> cat=`$path_private_rules`;
> err=`testresult $?`
> i=$?
> echo "Setting up private firewall rules ... $err"
>
> else
> # echo -e "No private firewall rules defined
...\033[40m\033[1;32mOK\033[0m"
> echo -e "No private firewall rules defined ...OK"
> fi;
>
>
> #-----
> # Logging
> #-----
> # All other incoming, forwarding and outgoing is denied and logged.
> $path_iptables -A INPUT -i $ext_if -s any/0 -d any/0 -j LDROP &&
> $path_iptables -A OUTPUT -o $ext_if -s any/0 -d any/0 -j LDROP &&
> $path_iptables -A FORWARD -o $ext_if -s any/0 -d any/0 -j LDROP &&
>
> # Set up LDROP
> $path_iptables -A LDROP -m state --state INVALID -j LOG --log-level
> info --log-prefix "State INVALID Dropped: " &&
>
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> $path_iptables -A LDROP -p tcp --tcp-flags ALL FIN,URG,PSH -m limit \  
> --limit 5/minute -j LOG --log-level notice --log-prefix "NMAP-XMAS: " &&  
> $path_iptables -A LDROP -p tcp --tcp-flags ALL FIN,URG,PSH -j DROP &&  
>  
> $path_iptables -A LDROP -p tcp --tcp-flags SYN,RST SYN,RST -m limit \  
> --limit 5/minute -j LOG --log-level notice --log-prefix "SYN/RST: " &&  
> $path_iptables -A LDROP -p tcp --tcp-flags SYN,RST SYN,RST -j DROP &&  
>  
> $path_iptables -A LDROP -p tcp --tcp-flags SYN,FIN SYN,FIN -m limit \  
> --limit 5/minute -j LOG --log-level notice --log-prefix "SYN/FIN: " &&  
> $path_iptables -A LDROP -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP &&  
>  
> $path_iptables -A LDROP -p tcp --tcp-flags ALL FIN -m limit \  
> --limit 5/minute -j LOG --log-level notice --log-prefix "FIN: " &&  
> $path_iptables -A LDROP -p tcp --tcp-flags ALL FIN -j DROP &&  
>  
> $path_iptables -A LDROP -p tcp --tcp-flags ALL ALL -m limit \  
> --limit 5/minute -j LOG --log-level notice --log-prefix "ALL/ALL: " &&  
> $path_iptables -A LDROP -p tcp --tcp-flags ALL ALL -j DROP &&  
>  
> $path_iptables -A LDROP -p tcp --tcp-flags ALL NONE -m limit \  
> --limit 5/minute -j LOG --log-level notice --log-prefix "NULL: " &&  
> $path_iptables -A LDROP -p tcp --tcp-flags ALL NONE -j DROP &&  
>  
> $path_iptables -A LDROP -p tcp -m limit --limit 1/s -j LOG --log-level  
> info --log-prefix "TCP_Dropped: " &&  
> $path_iptables -A LDROP -p udp -m limit --limit 1/s -j LOG --log-level  
> info --log-prefix "UDP_Dropped: " &&  
> $path_iptables -A LDROP -p icmp -m limit --limit 1/s -j LOG --log-level  
> info --log-prefix "ICMP_Dropped: " &&  
> $path_iptables -A LDROP -f -m limit --limit 1/s -j LOG --log-level  
> warning --log-prefix "FRAGMENT_Dropped: " &&  
> $path_iptables -A LDROP -j DROP  
> err=`testresult $?`  
> i=$?  
> echo "Enable logging ... $err";  
>  
> #  
> if [ "$i" -gt "0" ]  
> then  
> echo "Firewall error" >> /var/log/messages  
> # echo -e "$datum \033[40m\033[1;31mErrors detected in bringing up  
> firewall!\033[0m" | tee -a /var/log/messages  
> echo -e "$datum Errors detected in bringing up firewall!" | tee -a  
> /var/log/messages  
> # echo -e "$datum \033[40m\033[1;31mCheck your configuration.\033[0m" |  
> tee -a /var/log/messages  
> echo -e "$datum Check your configuration." | tee -a /var/log/messages  
> else  
> # echo -e "$datum \033[40m\033[1;32mFirewall is up without errors!\033[0m"  
|
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> tee -a /var/log/messages
> echo -e "$datum Firewall is up without errors!" | tee -a /var/log/messages
> echo;
> fi
>
> ;;
>
> stop)
> # ***** STOPPING FIREWALL *****
> echo;
> datum=`date +%b %d %k:%M:%S`;
> echo "$datum Shutting down firewall and masquerading" | tee -a
> /var/log/messages
> echo "$datum WARNING: YOUR MACHINE IS NOW OPEN FOR ATTACKS!!!" | tee -a
> /var/log/messages
> echo;
>
> # Remove all existing rules belonging to this filter
> $path_iptables -F
> $path_iptables -t nat -F
> $path_iptables -t mangle -F
>
> # Delete all user-defined chain to this filter
> $path_iptables -X
> $path_iptables -t nat -X
> $path_iptables -t mangle -X
>
> # Reset the default policy of the filter to accept.
> $path_iptables -P INPUT ACCEPT
> $path_iptables -P OUTPUT ACCEPT
> $path_iptables -P FORWARD ACCEPT
> $path_iptables -t nat -P POSTROUTING ACCEPT
> $path_iptables -t nat -P PREROUTING ACCEPT
> $path_iptables -t mangle -P OUTPUT ACCEPT
> $path_iptables -t mangle -P PREROUTING ACCEPT
>
>
> ;;
> restart)
> datum=`date +%b %d %k:%M:%S`;
> echo "$datum Firewall restart ..." | tee -a /var/log/messages
> $0 stop
> echo "-----"
> $0 start
>
>
> ;;
> status)
> $path_iptables -L -n --line-numbers
>
>
```

comp.security.firewalls: Re: Trouble accessing Outlook Web Access from behind firewall

```
> ;;  
> *)  
> # ***** WRONG PARAMETERS *****  
> echo;  
> echo "Wrong parameter input!"  
> echo "Usage: $0 {start/stop/restart/status}"  
> ;;  
> esac  
>  
>  
>  
>
```

---

- *Next message:* [mm: "Problems with watchguard muvpn & win2000"](#)
- *Previous message:* [Eirik Seim: "Re:](#)