

## Outpost Rules, Outpost rules for system & app

-----  
-----  
//////////\*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @  
TekGyd | itechhacks | Mukeshtricks4u\*////////  
-----  
-----

Here you can find how to set up your Outpost firewall. Most of this rules I found on the internet, but some of them are mine. I think that you should be safer.

I used the online tests to test my firewall settings. The links to these testers are:

### CODE

<http://scan.sygate.com/probe.html>  
<http://www.auditmypc.com/>  
<http://www.pcflank.com/about.htm>  
<https://grc.com/x/ne.dll?bh0bkyd2>  
<http://scan.sygatetech.com/>  
<http://security1.norton.com/>

### SYSTEM:

Allow DNS Resolving

Protocol: UDP

Remote Port(s): DNS (53)

Action: Allow It

Allow Outgoing DHCP

Protocol: UDP

Remote Port(s): bootps (67),  
bootp (68), dhcpv6-client (546),  
dhcpv6-server (547)

Action: Allow It

Allow Inbound Identification

Protocol: TCP

Direction: Inbound

Local Port(s): AUTH (113)

Action: Allow It

Allow Loopback

Protocol: TCP

Remote Host: localhost  
(127.0.0.1)

Action: Allow It

Allow GRE Protocol

Protocol: IP and the type is GRE  
(IP protocol 47)  
Action: Allow It

.  
Allow PPTP control connection  
Protocol: TCP  
Remote Port(s): PPTP  
Local Port(s): 1024-65535  
Action: Allow It

Block Remote Procedure Call  
(TCP)  
Protocol: TCP  
Direction: Inbound  
Local Port(s): DCOM(135)  
Action: Reject It

Block Remote Procedure Call  
(UDP)  
Protocol: UDP  
Direction: Inbound  
Local Port(s): 135  
Action: Reject It

Block Server Message Block  
Protocol (TCP)  
Protocol: TCP  
Direction: Inbound  
Local Port(s): Microsoft DS (445)  
Action: Reject It

Block Server Message Block  
Protocol (UDP)  
Protocol: UDP  
Direction: Inbound  
Local Port(s): Microsoft DS (445)  
Action: Reject It

APPLICATION

SVCHOST.EXE

Allowing DHCP  
Protocol: UDP  
LocalPort: 68  
RemotePort: 67  
Direction: Inbound  
AllowIt

Allowing DNS  
Protocol: UDP  
LocalPort: 53  
AllowIt

Time Synchronizer  
connection  
Protocol: UDP  
RemotePort: 123  
AllowIt

Allowing HTTP  
connection  
Protocol: TCP  
RemotePort: 80  
Direction:  
Outbound  
AllowIt

Allowing HTTPS  
connection  
Protocol: TCP  
RemotePort: 443  
Direction:  
Outbound  
AllowIt

Blocking "SSDP  
Discovery Service"  
and "UPnP device  
Host" services  
Protocol: UDP  
RemotePort: 1900  
RemoteHost: 239.255.255.250  
Direction: Inbound  
Reject It

Blocking "SSDP  
Discovery Service"  
and "UPnP device  
Host" services  
Protocol: TCP  
RemotePort: 5000  
RemoteHost: 239.255.255.250  
Direction: Inbound  
Reject It

Blocking "SSDP  
Discovery Service"  
and "UPnP device  
Host" services  
Protocol: UDP  
RemotePort: 5000  
RemoteHost: 239.255.255.250  
Direction: Inbound  
Reject It

Blocking "Remote  
Procedure Call"

Protocol: TCP  
Local port: 135  
Reject It

Web browsers:

Protocol: TCP  
Direction: Outbound  
Remote Port(s): HTTP(80), 81-83  
Action: Allow It

Protocol: TCP  
Direction: Outbound  
Remote Port(s): HTTPS(443)  
Action: Allow It

Protocol: TCP  
Direction: Outbound  
Remote Port(s): SOCKS (1080)  
Action: Allow It

Protocol: TCP  
Direction: Outbound  
Remote Port(s): 3128, 8080, 8088  
Action: Allow It

Protocol: TCP  
Direction: Outbound  
Remote Port(s): FTP(21)  
Action: Allow It

Protocol: TCP  
Direction: Inbound  
Remote Port(s): FTP DATA (20)  
Action: Allow It

Protocol: TCP  
Direction: Inbound  
Local Port(s): 1024- 65535  
Direction: Outbound  
Remote Port(s): 1024- 65535  
Action: Allow It

Protocol: TCP  
Direction: Inbound  
Remote Port(s): 1375  
Action: Allow It

Protocol: UDP  
Direction: Inbound  
Remote Port(s): 1040-1050  
Action: Allow It

E-Mail clients:

Protocol: TCP  
Direction: Outbound  
Remote Port(s): SMTP (25)  
Action: Allow It

Protocol: TCP  
Direction: Outbound  
Remote Port(s): NNTP (119)  
Action: Allow It

Protocol: TCP  
Direction: Outbound  
Remote Port(s): POP3 (110)  
Action: Allow It

Protocol: TCP  
Direction: Outbound  
Remote Port(s): IMAP (143)  
Action: Allow It

Protocol: TCP  
Direction: Outbound  
Remote Port(s): HTTP (80), 81-83, HTTPS (443), SOCKS (1080), 3128, 8080, 8088, 11523  
Action: Allow It

Antivirus updaters:

Protocol: TCP  
Direction: Outbound  
Remote Port(s): HTTP (80), 81-83, HTTPS (443), SOCKS (1080), 3128, 8080, 8088, 11523  
Action: Allow It  
Symantec LiveUpdate HTTP  
KAV Updater HTTP connection  
McAfee Update  
Update NOD32 virus definitions

Protocol: TCP  
Direction: Outbound  
Remote Port(s): FTP (21)  
Action: Allow It  
Symantec LiveUpdate FTP  
KAV Updater FTP connection

Protocol: TCP  
Direction: Inbound  
Remote Port(s): FTP DATA (20)  
Action: Allow It  
Symantec LiveUpdate FTP DATA  
KAV Updater FTP DATA connection

Protocol: TCP  
Direction: Outbound  
Remote Port(s): POP3 (110)  
Action: Allow It  
Scan incoming mail for viruses

#### Downloaders:

Protocol: TCP  
Direction: Outbound  
Remote Port(s): 80(HTTP), 81-83,  
443(HTTPS), 1080(SOCKS),  
3128, 8080, 8088, 11523  
Action: Allow It  
FlashGet, GerRight, Go!Zilla, ReGet

Protocol: TCP  
Direction: Outbound  
Remote Port(s): FTP (21)  
Action: Allow It  
FlashGet, GerRight, Go!Zilla, ReGet

Protocol: TCP  
Direction: Inbound  
Remote Port(s): FTP DATA (20)  
Action: Allow It  
FlashGet, GerRight, Go!Zilla, ReGet

Protocol: TCP  
Direction: Outbound  
Remote Port(s): 1024-65535  
Action: Allow It  
ReGet PASV FTP connection

Protocol: TCP  
Direction: Inbound  
Remote Port(s): 1024-65535  
Action: Allow It  
ReGet PASV FTP connection

Protocol: TCP  
Direction: Outbound  
Remote Port(s): 80, 3128, 8080,  
1080, 11523  
Action: Allow It  
ReGet Update

#### Trillian:

Trillian Pro Login  
Where the protocol is: TCP  
and Where the direction is: Outbound

and Where the remote host is: [www.ceruleanstudios.com](http://www.ceruleanstudios.com)  
and Where the remote port is: HTTP  
Action: Allow It

#### Trillian Pro AOL/ICQ Connection

Where the protocol is: TCP  
and Where the direction is: Outbound  
and Where the remote port is: 443, 5190  
Action: Allow It

#### Trillian mIRC AUTH Connection

Where the protocol is: TCP  
and Where the direction is: Inbound  
and Where the local port is: 113  
Action: Allow It

#### Trillian mIRC Connection

Where the protocol is: TCP  
and Where the direction is: Outbound  
and Where the remote port is: 6667  
Action: Allow It

#### Trillian MSN Connection

Where the protocol is: TCP  
and Where the direction is: Outbound  
and Where the remote port is: 1863  
Action: Allow It

#### Trillian Yahoo Connection

Where the protocol is: TCP  
and Where the direction is: Outbound  
and Where the remote port is: 5050  
Action: Allow It

#### Bit Torrent:

##### Bit Torrent HTTP Connection Rule

Where the protocol is: TCP  
and Where the direction is: Outbound  
and Where the remote port is: HTTP  
Action: Allow It

##### Bit Torrent HTTPS Connection Rule

Where the protocol is: TCP  
and Where the direction is: Outbound  
and Where the remote port is: 443  
Action: Allow It

##### Bit Torrent Network TCP Outbound Connection Rule

Where the protocol is: TCP  
and Where the direction is: Outbound  
and Where the remote port is: 1024 - 65535  
Action: Allow It

#### Bit Torrent Network TCP Inbound Connection Rule

Where the protocol is: TCP

and Where the direction is: Inbound

and Where the local port is: 6881-6999

Action: Allow It

#### TCP Inbound Coverage Rule

Where the protocol is: TCP

and Where the direction is: Inbound

Action: Reject It

#### TCP Outbound Coverage Rule

Where the protocol is: TCP

and Where the direction is: Outbound

Action: Reject It

#### UDP Coverage Rule

Where the protocol is: UDP

Action: Reject It

\* If you do not wish to share your files with others on the network you will need set this to Block It or leave it unchecked.